Naval Audit Service

Audit Report

Cyberspace/Information Technology Skill Sets for Active Duty Military Personnel at Selected Navy Commands

This report contains information exempt from release under the Freedom of Information Act. Exemption (b)(6) applies.

N2014-0021
19 May 2014

Obtaining Additional Copies

To obtain additional copies of this report, please use the following contact information:

Phone: (202) 433-5757
Fax: (202) 433-5921
E-mail: NAVAUDSVC.FOIA@navy.mil
Mail: Naval Audit Service
Attn: FOIA
1006 Beatty Place SE
Washington Navy Yard DC 20374-5005

Providing Suggestions for Future Audits

To suggest ideas for or to request future audits, please use the following contact information:

Phone: (202) 433-5840 (DSN 288)
Fax: (202) 433-5921
E-mail: NAVAUDSVC.AuditPlan@navy.mil
Mail: Naval Audit Service
Attn: Audit Requests
1006 Beatty Place SE
Washington Navy Yard DC 20374-5005

DEPARTMENT OF THE NAVY
NAVAL AUDIT SERVICE
1006 BEATTY PLACE SE
WASHINGTON NAVY YARD, DC 20374-5005

7510
2012-052
19 May 14

MEMORANDUM FOR DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER
DEPUTY CHIEF OF NAVAL OPERATIONS (INFORMATION DOMINANCE) (N2/N6)

Subj: **CYBERSPACE/INFORMATION TECHNOLOGY SKILL SETS FOR ACTIVE DUTY MILITARY PERSONNEL AT SELECTED NAVY COMMANDS (AUDIT REPORT N2014-0021)**

Ref: (a) NAVAUDSVC memo 7510 2012-052, dated 25 Jan 13
(b) SECNAV Instruction 7510.7F, "Department of the Navy Internal Audit"

1. The report provides results of the subject audit announced in reference (a). Section A of this report provides our findings and recommendations, summarized management responses, and our comments on the responses. Section B provides the status of the recommendations. The full text of management responses is included in the Appendices.

2. Department of the Navy Chief Information Officer concurred with Recommendations 1-4 and 10-11, and planned corrective actions meet the intent of the recommendations. Deputy Chief of Naval Operations (Information Dominance) (N2/N6) concurred with Recommendations 5- 9, and planned corrective actions meet the intent of the recommendations. Recommendations 1-9 are considered open pending completion of the planned corrective actions, and are subject to monitoring in accordance with reference (b). Management should provide a written status report on the recommendations within 30 days after target completion dates. Please provide all correspondence to the Principal Director for Internal Control and Investigative Support Audits, XXXXXXXXXXX, by e-mail, XXXXXXXXXXXX, with a copy to the Director, Policy and Oversight, XXXXX XXXXXXXXXXXXXXXXX. Please submit correspondence in electronic format (Microsoft Word or Adobe Acrobat file), and ensure that it is on letterhead and includes a scanned signature.

FOIA (b)(6)

FOIA (b)(6)

3. Any requests for this report under the Freedom of Information Act must be approved by the Auditor General of the Navy as required by reference (b). This audit report is also subject to followup in accordance with reference (b).

Subj: **CYBERSPACE/INFORMATION TECHNOLOGY SKILL SETS FOR ACTIVE DUTY MILITARY PERSONNEL AT SELECTED NAVY COMMANDS (AUDIT REPORT N2014-0021)**

4. We appreciate the cooperation and courtesies extended to our auditors.

[redacted]

FOIA (b)(6)

XXXXXXXXXXXXXX
Principal Director
Internal Control and Investigative
Support Audits

Copy to:
UNSECNAV
OGC
DCMO
ASSTSECNAV FMC
ASSTSECNAV FMC (FMO)
ASSTSECNAV EIE
ASSTSECNAV MRA
ASSTSECNAV RDA
CMC (DMCS, ACMC)
CNO (VCNO, DNS-33, N40, N41) (N4B)
VCNO
NAVINSGEN (NAVIG-14)
AFAA/DO

Table of Contents

Executive Summary

Overview

The Navy's Cyberspace/Information Technology Workforce (CS/ITWF) is deployed at over 3,000 locations within and outside the continental United States, including Hawaii, Cuba, Guam, Japan, and Puerto Rico. CS/ITWF members are military and Government civilians who plan for, budget for, manipulate, control, and archive information throughout its life cycle; develop, acquire, implement, evaluate, maintain, and retire information, information systems, and Information Technology; and develop and apply the necessary policies and procedures that protect and defend information and information systems.[1] The Department of the Navy (DON) CS/ITWF Strategic Plan for Fiscal Years (FY) 2010-2013 established DON priorities for ensuring workforce excellence. It identifies the goals and objectives that will allow DON to recruit, manage, develop, sustain, and retain a workforce for IT-related functions. DON CS/ITWF goals are to: (1) provide workforce capabilities that fully support cyberspace operations, (2) develop competency-based planning and management processes, (3) support required capabilities by recruiting a qualified and experienced workforce, and (4) develop and manage the DON Cybersecurity/Information Assurance Workforce.

The DON Chief Information Officer (DON CIO) is required to develop Cyberspace Workforce policy and guidance; invest resources to recruit, train, retain, and equip personnel for cyberspace missions; and track and measure the effectiveness of DON cyberspace manpower, personnel, training, and education programs. The Chief of Naval Operations is required to identify CS/ITWF positions and personnel, and to develop and implement the CS/ITWF Continuous Learning Program within the Navy.

We performed the audit between 11 December 2012 and 1 April 2014. Conditions existed at the time of our field work.

Reason for Audit

The objective of the audit was to verify that the internal controls over management of CS/ITWF skill sets were sufficient to ensure that Navy Cyberspace/IT active duty

[1] The cyber security/information assurance portion of the overall CS/ITWF workforce is the Information Assurance Workforce (personnel who have separate cybersecurity related training/certification requirements). They work to protect Department of the Navy (DON) information and systems from unauthorized access.

military personnel at selected commands were technically proficient in IT-related functions.

This audit was based on a risk area submitted by the Commander, Naval Education and Training Command and included in the Navy risk assessment for FYs 2007-2011 (it was not resubmitted in FY 2012 due to our planned audit). The concerns were that budget cuts, an aging workforce, and increasing Information Assurance (IA) compliance requirements make it harder to maintain a workforce with the technological skill sets needed for complete system maintenance and the production lifecycle in an ever-changing IT environment.

The audit focused on evaluating procedures and internal controls to ensure that sufficient CS/ITWF skill sets were maintained for active duty military personnel at selected shore and afloat subordinate activities under the Commander, U.S. Fleet Forces Command, Norfolk VA; the Commander, U.S. Fleet Cyber Command/U.S. 10th Fleet, Fort Meade, MD; and the Space and Naval Warfare Command, San Diego, CA.

Conclusions

We determined that the Navy did not have sufficient internal controls in place over management of CS/ITWF skill sets to ensure that active duty military personnel at selected commands were technically proficient in their IT-related functions.

Identification and Administration of the Navy CS/ITWF. DON did not have a clearly delineated CS/ITWF. Specifically, DON did not: (1) uniformly define the Navy's total CS/ITWF and identify which officer and enlisted personnel occupations comprised the CS/ITWF; (2) ensure the CS/ITWF definition was communicated to all levels within the Navy; and (3) establish an accurate, comprehensive database of all CS/ITWF military personnel. Our review found five sources that communicated to Navy CS/ITWF personnel who made up the CS/ITWF. These sources were not uniform and did not clearly and completely show which Navy Enlisted Classification Codes (NECs), Naval Officer Billet Codes (NOBCs), and Navy enlisted ratings comprise the Navy's total CS/ITWF. We also found that the activity personnel interviewed did not have a consistent understanding of who comprised the total CS/ITWF. The lack of a clearly identified CS/ITWF makes it difficult for DON and lower command levels to: recognize future needs of the total CS/ITWF, determine the proficiency and skill gaps for the CS/ITWF, and establish and track CS/ITWF training and education as required. These issues may impact readiness of fleet and shore activity active duty personnel.

Training of Navy CS/ITWF Personnel. DON did not provide training and certification guidance for the overall CS/ITWF as required. It also did not provide sufficient guidance

defining training for CS/ITWF line officers or provide pipeline training[2] for the Information Systems Technician/Information Systems Technician (Subsurface) (IT/ITS) ratings. At the 15 activities we visited, all 20 officers who we interviewed identified CS/ITWF skill gaps at the ship or activity levels. Five of the 20 officers stated that after completing the training currently available, they did not possess the skill sets required to adequately supervise the work of their CS/ITWF personnel.

We also found that 68 of the 96 enlisted personnel reviewed (71 percent) identified skill gaps. Overall, the personnel interviewed said they had sufficient skills to perform their daily tasks; however, there were instances where personnel stated they were provided training not relevant to their current tasks or were not provided formalized training for their current role. They also stated that they obtained training geared more towards passing certification exams versus being geared towards the fleet, and obtained very minimal, if any, practical training experience. Therefore, they said they did not have a full understanding of their roles and responsibilities.

Further, 30 of the 96 enlisted personnel interviewed (31 percent) stated they did not have appropriate skills to perform their IT-related functions. These individuals said they did not maintain a sufficient skill set to adequately perform their daily tasks and therefore, relied heavily on their peers. Additionally, CS/ITWF documentation to validate CS/ITWF training was not provided for 16 of the 116 officers and enlisted personnel reviewed. Documentation of training for the remaining 100 personnel was obtained from hard copies of documentation in the training jackets or from data found in the Fleet Management and Planning System (FLTMPS) and Total Workforce Management System (TWMS).[3] For the commands audited, 100 of 116 active duty personnel provided 191 source documents (i.e., hard copies of training certificates) for CS/ITWF-related training completed. Although commands entered data from 122 of the CS/ITWF-related training documents into FLTMPS, they did not enter information for 69 source documents. In addition, although commands entered data from 123 of the CS/ITWF-related training documents into TWMS, they did not enter data for 68 source documents.

As a result of the absence of guidance and insufficient officer and enlisted CS/ITWF training, fleet and shore activity readiness may be adversely affected. Also, line officers may lack the ability to oversee CS/ITWF-related staff, and the number of available active duty personnel with the technological skill sets needed for Cyberspace/IT work-roles may be limited. In addition, the absence of a centralized system with comprehensive training/certification records for the CS/ITWF makes it difficult for Navy commands to: (1) determine personnel proficiency and skill gaps; (2) use the workforce in the most

[2] Pipeline training is the control and supervision of movement or flow of students through the training pipeline. A pipeline provides accountability and helps maintain the uninterrupted flow of students (Naval Education Training Manual, 135C, Chapter 3, Section 1, Paragraph 1.1).
[3] FLTMPS and TWMS are two systems that maintain electronic records showing training completed and certifications earned for active duty military members.

efficient and effective manner; and (3) establish and track training, manpower, and continuing education requirements as required.

Department of the Navy Managers' Internal Control Program. Fourteen of 15 activities we reviewed did not include the CS/ITWF in their assessable units for the FY 2013 Managers' Internal Control Program at the activity or higher command levels. If CS/ITWF is not included in assessable units in command Managers' Internal Control Programs, there is no assurance that internal controls are evaluated in this area as required or any material weaknesses noted are reported to higher levels. This can lead to the ineffective use of limited resources (both personnel and funds). The lack of documented oversight can have an impact on mission readiness.

Communication with Management. Throughout the audit, we kept personnel at the DON CIO, the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) and the leadership of the commands we visited, informed about our findings. Specifically, we briefed DON CIO on 17 April 2013 and 1 July 2013. We briefed OPNAV N2/N6 on 5 June 2013. We held a status brief with: the N1 Captain and N6 Captain, U.S. Fleet Forces Command, Norfolk, VA on 9 December 2013; Executive Director, U.S. Fleet Cyber Command/U.S. 10th Fleet, Fort Meade, MD on 11 December 2013; Director-Total Force Management, Space and Naval Warfare System Command San Diego, CA on 19 December 2013; the Commanding Officer, Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT), Norfolk, VA on 13 February 2013; and the Chief Information Officer, Naval Education and Training Command on 14 August 2013.

Federal Managers' Financial Integrity Act

The Federal Managers' Financial Integrity Act (FMFIA) of 1982, as codified in Title 31, United States Code, requires each Federal agency head to annually certify the effectiveness of the agency's internal and accounting system controls. Recommendations 1 through10 address issues related to the internal controls over management of the Navy's active duty personnel Cyberspace/Information Technology skill sets. In our opinion, the weaknesses noted in this report may warrant reporting in the Auditor General's annual FMFIA memorandum identifying management control weaknesses to the Secretary of the Navy.

Corrective Actions

We made recommendations to the Department of the Navy Chief Information Officer and Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) to address the issues noted.

We recommended that the Department of the Navy Chief Information Officer:

- Develop and issue guidance to convey to the members of the Department of the Navy Cyberspace/Information Technology Workforce their inclusion and role within the Cyberspace/Information Technology workforce structure;
- Establish workforce requirements to identify and track positions, personnel, and qualifications within the Cyberspace/Information Technology Workforce;
- Establish and maintain a comprehensive personnel database to capture all personnel who comprise the Department of the Navy Cyberspace/Information Technology Workforce;
- Develop and issue training and certification guidance for the overall Cyberspace/Information Technology Workforce;
- Require that all Navy commands with Cyberspace/Information Technology Workforce personnel include Cyberspace/Information Technology Workforce in their assessable units under their Managers' Internal Control Programs and perform and document internal control evaluations for these assessable units using existing sources or separate evaluations, as required; and
- Ensure that management at all afloat activities are aware of their responsibilities for establishing, evaluating, and improving internal controls for the Cyberspace/Information Technology Workforce under the Managers' Internal Control Program.

We recommended that the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6):

- Redefine training requirements and oversight for Cyberspace/Information Technology Workforce line officers to ensure that they have the education and competencies needed to support the Department of the Navy's mission, goals, and dynamic workforce structure changes;
- Ensure IT/ITS Cyberspace/Information Technology Workforce enlisted personnel have pipeline training and career development reflecting their current set of competencies;
- Establish a centralized system to track and maintain a complete training history for Cyberspace/Information Technology Workforce personnel;
- Establish procedures and related internal controls requiring that electronic or hard copy training records and certifications be retained for all Cyberspace/Information Technology Workforce active duty military members; and
- Until the centralized system is established, establish procedures and related internal controls requiring that all Cyberspace/Information Technology Workforce

training records and certifications be recorded/entered into the Fleet Management and Planning System or Total Workforce Management System.

The management took or plans appropriate corrective actions for all of the recommendations.

Section A:

Findings, Recommendations, and Corrective Actions

Finding 1: Identification and Administration of the Navy Cyberspace/Information Technology Workforce

Synopsis

The Department of the Navy (DON) did not have a clearly delineated Cyberspace/Information Technology Workforce (CS/ITWF) as required by Secretary of the Navy (SECNAV) guidance. Specifically, DON did not:

- Uniformly define the Navy's total CS/ITWF and identify which officer and enlisted personnel occupations comprised the CS/ITWF;
- Ensure the CS/ITWF definition was communicated to all levels within the Navy; and
- Establish an accurate, comprehensive database of all CS/ITWF military personnel.

The DON Chief Information Officer (DON CIO) is required to develop Cyberspace Workforce policy and guidance; and to track and measure the effectiveness of DON cyberspace manpower, personnel, training, and education programs. The Chief of Naval Operations is required to identify CS/ITWF positions and personnel.

Responsible Navy personnel informed us that the above deficiencies occurred because:

- Navy management placed CS/ITWF-related emphasis on identifying and developing the Navy's Information Assurance Workforce[4] in accordance with the Federal Information Security Management Act of 2002 (FISMA) and Department of Defense (DoD) standard requirements;
- DON could not comprehensively define the overall CS/ITWF or develop a CS/ITWF personnel database because related standard DoD procedures had not been established yet; and

[4] The cybersecurity/information assurance portion of the overall CS/ITWF workforce is the Information Assurance Workforce (personnel who have separate cybersecurity-related training/certification requirements).

- Dynamic workforce structure changes continually impact the description, identification, and development of active duty personnel supporting cyber operations.

However, due to the criticality of the CS/ITWF in achieving DON objectives in every warfighting domain and enterprise business model, as discussed in SECNAV Instruction 3052.2, "Cyberspace Policy and Administration within DON," as well as the following potential impacts; a CS/ITWF definition and related database of on-hand CS/ITWF personnel needs to be developed. As a result, in our opinion, the lack of a clearly identified CS/ITWF inhibits DON and lower command levels' ability to: recognize the future training needs of the total CS/ITWF; determine where proficiency and skill gaps exist for the CS/ITWF; and establish and track CS/ITWF manpower personnel, training, and education as required. All of these issues may impact readiness of fleet and shore activity duty personnel.

Discussion of Details

Background

The CS/ITWF is deployed at over 3,000 locations in the continental United States, as well as Hawaii, Cuba, Guam, Japan, and Puerto Rico. The CS/ITWF assists in the engineering, design, development, installation, operation, servicing, and restoration of computer networks, systems, and applications. They also continuously work to protect DON information and systems from unauthorized access. The workforce operates on the Navy Marine Corps Intranet (NMCI) across the continental United States, on the OCONUS (outside continental United States) Navy Enterprise Network (ONE-NET) at shore installations overseas, and through the Information Technology for the 21st Century (IT-21), which provides networking capabilities to the fleet.

The Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) Zero-Based Review Task Force database (verified by the Task Force based on database review by Navy commands), as of 18 October 2012, identified 27,405 authorized Navy CS/ITWF billets,[5] of which 16,075 (59 percent) were military personnel. The universe for our audit was the 15,897 active duty military personnel (99 percent of the 16,075) (see Finding 2). Active duty and Reserve military personnel, civilians, and an extensive contractor workforce all perform critical Cyberspace/IT roles. The Information Assurance Workforce (IAWF), a subset of the total CS/ITWF, crosses Cyberspace/IT role boundaries and plays a critical role in cybersecurity (see Figure 1). As noted, the

[5] The Navy had not established a comprehensive database of on-hand CS/ITWF military personnel. Although this Zero-Based Review database only showed authorized billets, it was the most comprehensive record available to identify the total CS/ITWF.

Cybersecurity/Information Assurance portion of the overall CS/ITWF workforce is the IAWF (personnel who have separate cybersecurity-related training/certification requirements).

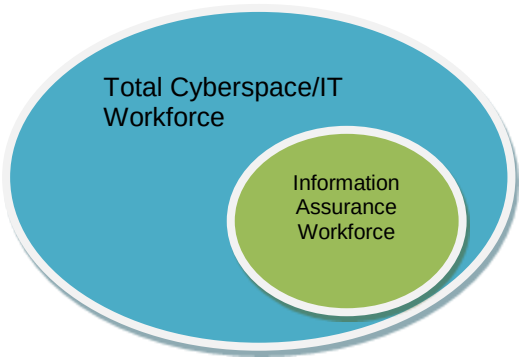


Figure 1. Relationship between IAWF and CS/ITWF.

Our audit focused on active duty officer and enlisted members of the Navy's total CS/ITWF at selected United States Navy commands.

Pertinent Guidance

SECNAV Instruction 3052.2, "Cyberspace Policy and Administration within DON," dated 6 March 2009, states that cyberspace capabilities are critical to achieving DON objectives in every warfighting domain and enterprise business model. Cyberspace operations will require intensive training and education for the total DON Cyberspace Workforce. It also states that the DON workforce will be a single integrated resource that is carefully managed with a dedicated focus on continued training and education to meet emerging technical developments and employed to provide the highest level of cyberspace capabilities to meet Naval and joint objectives. DON CIO shall develop required Cyberspace Workforce policy and guidance. With the DoD CIO and Assistant Secretary of the Navy (Manpower and Reserve Affairs), DON CIO will track and measure the effectiveness of DON cyberspace manpower, personnel, training, and education programs.

SECNAV Instruction 1543.2, "Cyberspace/Information Technology Workforce Continuous Learning," dated 30 November 2012, states that its purpose is to establish policy and procedures for DON CS/ITWF professional development through a Continuous Learning Program. This program is structured to support the continuing professional development of CS/ITWF personnel throughout their careers. The program will include education, training, certification and other activities that support the sustainment and continued improvement of the capabilities of the DON CS/ITWF. The overarching goal of the program is to improve cyberspace operations, cyberspace mission

effectiveness and increase readiness across the cyberspace domain. Specific related responsibilities are shown in Exhibit A.

The instruction defines the CS/ITWF as military and Government civilians who: plan, budget, manipulate, control and archive information throughout its life cycle; develop, acquire, implement, evaluate, maintain and retire information, information systems and IT; develop the necessary policies and procedures; and apply measures that protect and defend information and information systems.

Audit Results

DON did not have a clearly delineated CS/ITWF. Specifically, DON did not:

- Uniformly define the Navy's total CS/ITWF and identify which officer and enlisted personnel occupations comprised the CS/ITWF;
- Ensure the CS/ITWF definition was communicated to all levels within the Navy; and
- Establish an accurate, comprehensive database of all CS/ITWF military personnel.

As a result, in our opinion, the lack of a comprehensive uniform DON-wide CS/ITWF definition and related database of on-hand CS/ITWF personnel inhibits DON and lower command levels' ability to: (1) recognize future needs of the total CS/ITWF; (2) determine the proficiency and skill gaps for the CS/ITWF; and (3) establish and track CS/ITWF performance concerning manpower personnel, training, and education as required. All of these may impact readiness.

CS/ITWF Definition

DON did not uniformly define the Navy's total CS/ITWF and identify which officer and enlisted personnel occupations comprised the CS/ITWF, or ensure the CS/ITWF definition was communicated to all levels within the Navy. According to SECNAV Instruction 3052.2, "Cyberspace Policy and Administration within DON," DON CIO is required to develop Cyberspace Workforce policy and guidance, as well as track and measure the effectiveness of DON cyberspace manpower, personnel, training, and education programs.

To determine relevant criteria defining the total CS/ITWF and identify what military occupations comprise this workforce, we reviewed DON Web sites, prior years' cyber-related audit reports, and the DON Cyber/IT Workforce Strategic Plan. We also interviewed DON personnel at various commands. For our detailed scope and methodology, see Exhibit B.

Based upon our review, we found five sources which communicated to the Navy personnel who make up the CS/ITWF:

1. A 27 March 2008 article from the DON CIO Web site.
2. "DON Cyber/IT Workforce Strategic Plan FY 2010-2013," published July 2010.
3. SECNAV Instruction 1543.2, "Cyberspace/Information Technology Workforce Continuous Learning," dated 30 November 2012.
4. Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) Zero-Based Review Report, dated April 2012.[6]
5. Navy Credentialing Opportunities Online (COOL) Web site.[7]

These sources were not consistent with each other, and did not clearly and completely show which Navy Enlisted Classification Codes (NECs), Naval Officer Billet Codes (NOBCs) and Navy Enlisted ratings comprise the Navy's Total CS/ITWF. The only official Navy definition of who makes up the overall CS/ITWF, SECNAV Instruction 1543.2, "Cyberspace/Information Technology Workforce Continuous Learning," dated 30 November 2012, was not as comprehensive as other sources because it only identified two Navy enlisted ratings and four NOBCs for the CS/ITWF that qualify for professional development through a continuous learning program. Details on who the sources show as making up the CS/ITWF are shown in Exhibit D. Exhibit D shows that all five sources provide different narrative descriptions as to who is included in the CS/ITWF (i.e., each source describes CS/ITWF functions differently). Furthermore, two of the five sources do not identify actual billets/classifications/ratings included in the CS/ITWF.

Of the remaining three sources, as noted, SECNAV Instruction 1543.2 identifies two Navy Enlisted Ratings and four NOBCs for the CS/ITWF. The Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) Zero-Based Review Report includes NOBCs, NECs, and enlisted ratings shown in SECNAV Instruction 1543.2, as well as 20 additional NOBCs, 38 additional NECs[8] and 22 additional enlisted ratings. The Navy COOL Web site shows the same four NOBCs as SECNAV Instruction 1543.2; the same two Navy enlisted ratings as SECNAV Instruction 1543.2, as well as five more Navy enlisted ratings, totaling seven Navy enlisted ratings; as well as 33 NECs. So all of the three sources show different figures as to who makes up the CS/ITWF. The Navy needs a single source showing who comprises the CS/ITWF.

[6] The report's purpose section states, "Given the critical importance of building and maintaining a proficient and resilient cyber workforce, the Navy-wide Cyber Zero-Based Review was initiated in September 2011 to establish a baseline of the Navy's current cyber workforce based on present requirements and inform the development of an executable Cyber Warfare Manpower Strategy."

[7] Navy COOL is a Web site, designed for Navy service members, that defines civilian credentials that best map to Navy ratings, jobs, designators, and collateral duties/assignments. It outlines the path, work, training, and experience required to achieve them. It defines comprehensive information on occupational credentials — including certifications, licenses, apprenticeships, and growth opportunities — correlating with every Navy rating, job, designator, and collateral duty/out-of-rate assignment.

[8] The Continuous Learning criteria did not list any NECs as being part of the CS/ITWF.

As we performed our 15 activity visits, activity personnel gave different accounts as to who they said comprised the total CS/ITWF. When activities were asked to provide us with a complete list of their CS/ITWF personnel prior to the site visit, five activities provided personnel rosters that included only personnel from the Information Systems Technician (IT) or Information Systems Technician (Subsurface) (ITS) ratings. We noted that the term "CS/ITWF" did not have the same meaning for each activity. This showed us that the personnel within the Navy were generally unaware of who comprised the total CS/ITWF. In three instances, some personnel thought that only the IT/ITS ratings comprised the total CS/ITWF; whereas, others thought the Information Assurance Workforce was the total CS/ITWF.

Database of Total On-Hand CS/ITWF Personnel

DON did not establish an accurate, comprehensive database of all CS/ITWF military personnel as required by SECNAV Instruction 1543.2. To determine whether a comprehensive database of on-hand Navy CS/ITWF personnel was available, we interviewed personnel from DON CIO; the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6); the Bureau of Naval Personnel; and the Navy Manpower Analysis Center, Naval Personnel Command. We found that such a database did not exist. Our review of the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) Zero-Based Review Task Force database, in conjunction with discussions with management personnel from DON CIO, Zero-Based Review Task Force, and Navy Cyber Forces Command, showed the validated database was the most comprehensive record available to identify the total CS/ITWF. However, it only showed authorized billets, not on-hand personnel.

DON Rationale Concerning CS/ITWF Definition and CS/ITWF Database Development

We interviewed knowledgeable DON personnel to determine why DON did not: uniformly define the Navy's total CS/ITWF and identify which officer and enlisted personnel occupations comprised the CS/ITWF; ensure the CS/ITWF definition was communicated to all levels within the Navy; and establish an accurate, comprehensive database of all CS/ITWF military personnel. We interviewed personnel from: DON CIO; the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) Zero-Based Review Task Force; the Bureau of Naval Personnel; Navy Manpower Analysis Center, Naval Personnel Command; Navy Cyber Forces Command; and Naval Computer and Telecommunications Area Master Station Atlantic. The consensus based on these interviews was that these conditions occurred for the following reasons:

Navy Information Assurance Workforce Emphasis. DON CIO emphasized

identifying and developing the Navy's Information Assurance Workforce[9] (IAWF) in accordance with the Federal Information Security Management Act of 2002 (FISMA) and DoD standard requirements and did not have sufficient resources to identify and develop both the IAWF and the CS/ITWF.

Lack of Standard DoD CS/ITWF-Related Procedures. DON CIO personnel informed us that the Navy did not comprehensively define the overall CS/ITWF or develop a CS/ITWF personnel database because they were waiting for DoD to issue its guidance. We were told that DoD was drafting Directive 8140.aa, "Cyberspace Workforce Management," reissuing and renumbering DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," updating and expanding policies, and assigning responsibilities for managing the DoD workforce performing cyberspace functions.

DON CIO personnel stated that the current official Navy definition of who makes up the overall CS/ITWF, SECNAV Instruction 1543.2, represents the core personnel the Navy believes should clearly be included in the CS/ITWF, pending the draft DoD guidance. However, as noted above, this guidance is inconsistent with and not as complete as other sources which communicated to Navy personnel who were included in the CS/ITWF. DoD guidance will establish standard requirements that the Navy will implement concerning defining, identifying, and tracking CS/ITWF personnel.

Dynamic Workforce Structure Changes. DoD continues to institute dynamic force structure changes within the IT/Cybersecurity environment in response to a rapidly escalating threat to U.S. national security. The Office of the Secretary of Defense, the Joint Staff, Combatant Commanders, and the Military Services all acknowledge that as the cyber domain evolves to address current and emerging threats, the workforce roles will also evolve to position the Department to address the continuing evolving threats and missions of the Department. These changes continually impact the description, identification, and development of active duty personnel supporting cyber operations,[10] making it difficult to determine who to include when defining the CS/ITWF.

However, due to the criticality of the CS/ITWF in achieving DON objectives in every warfighting domain and enterprise business model, as discussed in SECNAV Instruction 3052.2, "Cyberspace Policy and Administration within DON," as well as the potential impacts discussed below, a CS/ITWF definition and related database of on-hand CS/ITWF personnel need to be developed.

Impact on the DON CS/ITWF

[9] The cybersecurity/information assurance portion of the overall CS/ITWF workforce is the Information Assurance Workforce (personnel who have separate cybersecurity related training/certification requirements).
[10] "Department of Defense Cyber Operation Personnel Report: Report to the Congressional Defense Committees As Required by Public Law 111-84, Paragraph 1, "Composition of the DoD Cyber Operations Workforce," dated April 2011.

DON cannot ensure that the right CS/ITWF personnel have the right training and experience without a comprehensive uniform Navy-wide CS/ITWF definition and related database of on-hand CS/ITWF personnel. This condition prevents CS/ITWF managers from collecting workforce metrics that ensure competencies and skills are visible to Cyber/IT leadership. In our opinion, the lack of training and experience of the CS/ITWF personnel may impact readiness of fleet and shore activities. The lack of knowledge concerning who comprises the CS/ITWF makes it difficult for DON and lower command levels to:

- Recognize future training needs of the total CS/ITWF and develop plans to meet those needs;
- Determine where proficiency and skill gaps exist for on-hand CS/ITWF personnel and develop plans to mitigate the gaps; and
- Establish and track CS/ITWF manpower, personnel, training, and education as required.[11]

Each CS/ITWF professional needs to have the tools and capabilities to be an effective cyber warfighter, sustain a robust capability in cyberspace, and achieve enterprise business objectives within the Naval networking environment. In our opinion, without complete, clearly articulated, and communicated guidance for the entire CS/ITWF, DON may have difficulty in achieving command and control of its cyber forces globally and in building unity in carrying out cyberspace operations.

DON CIO is required to track and measure the effectiveness of DON cyberspace manpower, personnel, training, and education programs, as well as identify measures for the evaluation of CS/ITWF continuous learning. The Chief of Naval Operations is required to evaluate Continuous Learning Program effectiveness and compliance through assessments and formal Inspector General inspections. Also, the DON CIO FY 2010-2013 strategic plan states that CS/ITWF managers should collect workforce metrics for purposes that include ensuring that competencies and skills are visible to Cyber/IT leadership. In our opinion, these tasks cannot be accomplished without a comprehensive, uniform Navy-wide CS/ITWF definition and related database of total on-hand CS/ITWF personnel.

Recommendations

We recommend that the Department of the Navy Chief Information Officer:

[11] Finding 2 provides additional details on skill gaps and training issues.

Recommendation 1. Develop and issue guidance to convey to the members of the DON Cyberspace/Information Technology Workforce their inclusion and role within the Cyberspace/Information Technology Workforce structure. At a minimum, this guidance should:

- Include all necessary information to ensure even the most junior personnel of the Cybersecurity and remaining Cyberspace/Information Technology Workforce understand that they comprise the overall Cyberspace/Information Technology Workforce.
- Require that this guidance be communicated to all levels within the Department of the Navy.

Department of Navy Chief Information Officer response to Recommendation 1. Concur. Future Department of Defense (DoD) and Department of the Navy (DON) policy and guidance will address the overall "Cyberspace Workforce" in total. The DoD definitions for the Cyberspace Workforce are not approved. In the draft DoD Directive 8140.aa, DoD defines the "Cyberspace/Information Technology Workforce [CS/ITWF]" as a subset of the overall "Cyberspace Workforce." Additionally, the Navy has established the Information Dominance Corps (IDC), which is a focused, mature workforce structure that clearly establishes a professional community. The DON Chief Information Officer (DON CIO) will work with the Navy to ensure that personnel understand their role in the Cyberspace Workforce through the issuance of revised DON policy. The DoD Directive 8140 should be released in the near future. The DON guidance will be promulgated by 30 September 2014.

Naval Audit Service comments on response to Recommendation 1. Actions planned by management to (1) issue DON policy and guidance to define the overall Cyberspace Workforce in total and ensure that Navy personnel understand their roles in the Cyberspace Workforce, and (2) have the IDC continue to establish a professional community, meet the intent of the recommendation. This recommendation is considered open pending completion of agreed-to actions.

Recommendation 2. Establish workforce requirements to identify and track positions, personnel, and qualifications within the Cyberspace/Information Technology Workforce.

Department of the Navy Chief Information Officer response to Recommendation 2. Concur. DON is in the process of coding Cyberspace and Cybersecurity positions as directed by Office of Personnel Management (OPM)

memo of 8 July 2013, "Special Cybersecurity Workforce Project" and DoD CIO memo of 27 Feb 2014, "Coding of DoD Cyberspace Management & IT/IM Workforce" (CI0000144-14). Additionally, the DON CIO is working with the Navy and Marine Corps to determine what information is required to properly identify and track Cyberspace Workforce positions and personnel. The Assistant Secretary of the Navy, Manpower and Reserve Affairs (ASN (M&RA)), the Deputy Assistant Secretary of the Navy for Civilian Human Resources (DASN (CHR)), DON CIO, and the Navy and Marine Corps are working together to ensure that manpower and personnel requirements and guidance are part of this effort. The guidance establishing CS/ITWF requirements to identify and track positions, personnel, and qualifications within the CS/ITWF will be promulgated by 30 September 2014.

Naval Audit Service comments on response to Recommendation 2. Actions planned and in process by management to (1) code Cyberspace and Cybersecurity positions; (2) determine what information is required to properly identify and track Cyberspace Workforce positions and personnel; and (3) issue guidance establishing CS/ITWF requirements to identify and track positions, personnel, and qualifications within the CS/ITWF, meet the intent of the recommendation. The recommendation is considered open pending completion of agreed-to actions.

Recommendation 3. Establish and maintain a comprehensive personnel database to capture all personnel who comprise the Department of the Navy Cyberspace/Information Technology Workforce based on the established workforce requirements. As a subset, this capability must provide the ability to identify and track personnel and positions that perform Cybersecurity functions.

Department of the Navy Chief Information Officer response to Recommendation 3. Concur. Both the Navy and the Marine Corps already have authoritative personnel databases for military positions and personnel. Civilian personnel information is maintained in the Defense Civilian Personnel Data System (DCPDS). DON CIO is working with ASN (M&RA), DASN (CHR), Navy, and Marine Corps to identify the most appropriate means and database for documenting CS/ITWF positions and personnel information. The Navy will continue to use the capabilities of the Total Workforce Management System (TWMS) to track Cyberspace and Cybersecurity unique data elements (those data elements not included in authoritative manpower and personnel data bases) as necessary. The Navy and Marine Corps are currently working with TWMS to modify and add more Cybersecurity data fields to meet future needs. Target date for completion is 31 December 2014.

Naval Audit Service comments on response to Recommendation 3. Actions planned by management meet the intent of the recommendation. The recommendation is considered open pending completion of agreed-to actions.

Finding 2: Training of Navy Cyberspace/IT Workforce Personnel

Synopsis

Although 81, or 70 percent, of the 116 active duty Navy CS/ITWF personnel reviewed said that they had sufficient training to perform their required duties, 5 officers and 30 enlisted personnel said they did not. Also, 88 active duty personnel believe IT skill gaps exist at their ship or activity. In addition, although training documentation was provided for 100 CS/ITWF personnel reviewed, documentation was not retained or available for 16 CS/ITWF personnel. Some CS/ITWF personnel were not sufficiently trained, and IT skill gaps existed because DON did not:

- Provide training and certification guidance for the overall CS/ITWF as required;
- Provide sufficient guidance defining required training for CS/ITWF line officers; or
- Provide pipeline training[12] for all enlisted members in the Information Systems Technician/Information Systems Technician (Subsurface) (IT/ITS) ratings.

Although DON has various systems[13] that capture some incomplete training information and documentation, DON did not have a centralized system or related procedures and internal controls to retain training and certification records for all CS/ITWF active duty members. Lack of sufficient officer and enlisted CS/ITWF training may impact fleet and shore activity readiness and impair oversight of the CS/ITWF. In addition, the absence of a centralized system to capture training documentation makes it difficult for Navy commands to determine personnel proficiency and skill gaps, use the workforce in the most efficient and effective manner, and establish and track training, manpower, and continuing education requirements as required.

[12] This term refers to the control and supervision of movement or flow of students through the training pipeline. A pipeline provides accountability and helps maintain uninterrupted flow of students.
[13] These systems include Fleet Management and Planning System (FLTMPS) and Total Workforce Management System (TWMS).

Discussion of Details

Pertinent Guidance

According to the DON Cyber/IT Workforce Strategic Plan for FYs 2010-2013, developing the CS/ITWF necessitates defining the required education and competencies needed to support DON's mission, goals, and dynamic workforce structure changes. According to Naval Personnel Manual (NAVPERS) 15839I, "Manual of Navy Officer Manpower and Personnel Classifications," Volume I, "Major Code Structures," dated January 2013, the Navy has two cyber operations designator codes for officers: 1820 -- Information Professional (IP) and 1840 -- Cyber Warfare Engineer. In addition to these officer communities, the Navy has Communications and Systems Officers in both the Limited Duty Officer (LDO) 6420 designator and Chief Warrant Officer 7420 designator communities. The manual explains that officers serving in the IP community provide expertise in information, command and control, and space systems through the planning, acquisition, operation, maintenance, and security of systems. It further explains that the Cyber Warfare Engineer duties include: applying Information Operations (IO) and signal intelligence expertise, leading IO personnel and advising commanding officers, coordinating information warfare measures in exercises and operations, and processing real-time signal intelligence. The differences in the roles of Warrant Officers and LDOs are subtle, but both require a breadth of expertise. Additional Pertinent Guidance is shown in Exhibit A.

Scope

We judgmentally selected 3 U.S. Fleet Forces Command and 2 Space and Naval Warfare Systems Command subordinate shore activities, along with 10 Navy ships for detailed test work. Within these 15 activities and ships, we judgmentally selected 20 officers with cyber operations designator codes and 96 enlisted personnel with CS/ITWF ratings or Navy Enlisted Classification codes to determine if CS/ITWF personnel at the activities and ships were properly trained at the time of our site visit. We also requested training documentation for the 116 selected officers and enlisted personnel. Details of our process for judgmentally selecting the 15 activities and ships, and 116 personnel are shown in Exhibit B.

Methodology

To identify relevant cyberspace operations training and certification guidance, we reviewed:

- The DON DON CIO and Navy Personnel Command Web sites;
- Cyberspace-related audit reports published from 2009 through 2011 by the Government Accountability Office, Department of Defense Inspector General, and Naval Audit Service;
- Several DoD and DON workforce-related criteria[14]; and
- PowerPoint presentations from the DON CIO 2012 Information Technology East Coast Conference.

We also interviewed personnel from the offices of the DON CIO, OPNAV, and the Navy Cyber Forces Command to obtain their opinions on whether the Navy is providing the necessary training to active duty CS/ITWF personnel to ensure that they are technically proficient in their IT-related functions.

The 96 enlisted personnel were interviewed to determine whether they and personnel at their activity or ship had the necessary skill sets to perform the minimum skill and knowledge requirements stated in the Naval Personnel Command (NAVPERS) 18068F, "Manual of Navy Enlisted Manpower and Personnel Classifications and Occupational Standards," Volumes I and II, dated April 2013 and January 2013, respectively. The 20 officers were interviewed to determine whether they or personnel on board their ship had the necessary skill sets to perform the minimum skill and knowledge requirements stated in OPNAV Instruction 3120.32D, "Standard Organization and Regulations Manual (SORM)," dated 16 July 2012. Exhibit B shows the detailed methodology/sources of data we used to prepare for and conduct these reviews. We requested a copy of the training and certification documentation for each individual selected for review to determine whether the individual reviewed was provided with and successfully completed the training necessary to perform their current CS/ITWF-related functions.[15] We compared the training and certification documentation obtained to the data contained in TWMS and FLTMPS to ensure the information was recorded accurately.

We reviewed the training documentation to identify the titles of the courses completed by the selected officers and enlisted personnel. The course titles allowed us to determine the overall type of relevant IT training received. We did not obtain course curriculums to fully evaluate the length and breadth of the training course, since the course title allowed us to discern if the training was general IT training or specialized training.

[14] See Exhibit B, Scope and Methodology, for a list of the guidance we reviewed, and Exhibit A, Pertinent Guidance, for the guidance.

[15] We accepted the following as valid source records for training taken and certifications earned for CS/ITWF active duty military members. Concerning electronic records for CS/ITWF-related training, we accepted (1) courses taken online on Navy Knowledge On-line (NKO) and TWMS, since course completion is automatically recorded on the systems when courses are successfully completed; and (2) courses other than those taken on-line (e.g., vendor courses, for which successful course completion/any resulting certifications were recorded in FLTMPS, TWMS, and Navy Training Management Planning System (NTMPS), three systems which maintain electronic records showing training completed and certifications earned for active duty military members). Concerning hard copy records for CS/ITWF-related training, we accepted hard copy records of successful training completion for any course that should have been input to systems such as FLTMPS or TWMS, but was not (a condition noted above), or any other CS/ITWF-related course taken.

Audit Results

Overall, although 81 (70 percent) of the 116 active duty Navy Cyberspace/IT Workforce (CS/ITWF) personnel reviewed said that they had sufficient training to perform their required duties, 5 officers and 30 enlisted personnel (totaling 30 percent of the 116 personnel) said they did not. Also, 88 (76 percent) of the 116 active duty personnel believed IT skill gaps exist at their ship or activity, and 71 (61 percent) of the 116 personnel believed that the IT function was undermanned. In addition, although training documentation was provided for 100 (86 percent) of the 116 CS/ITWF personnel reviewed, documentation was not retained or available for 16 (14 percent) of the 116 CS/ITWF personnel. CS/ITWF personnel were not sufficiently trained, and IT skill gaps existed because DON did not:

- Provide training and certification guidance for the overall CS/ITWF as required;
- Provide sufficient guidance defining required training for CS/ITWF line officers; or
- Provide pipeline training[16] for the IT/ITS ratings.

Although DON has various systems[17] that capture some training information and documentation, DON did not have a centralized system or related procedures and internal controls to retain training and certification records for all CS/ITWF active duty members.

Training and Certification Guidance

Although the Navy and DoD provided eight criteria related to cyberspace operations personnel, none of the criteria provided clear and comprehensive guidance for the training, certification, and development of the entire CS/ITWF. SECNAV Instruction 3052.2, "Cyberspace Policy and Administration within the DON," dated 6 March 2009, addressed the overarching responsibilities for the administration of the CS/ITWF. The DON Cyber/IT Workforce Strategic Plan FY 2010-2013 identified DON's goals and objectives for ensuring workforce excellence. SECNAV Instruction 1543.2, "Cyberspace/IT Workforce Continuous Learning," dated 30 November 2012, established policy in support of the continuing professional development of the CS/ITWF. Five of the eight criteria provided robust guidance specifically for the training, certification, and management of DoD's Information Assurance Workforce (IAWF). None of the eight criteria provided detailed training, certification, and development requirements for the entire CS/ITWF. Specifically, SECNAV Instruction 3052.2 (see Exhibit A) and the

[16] Pipeline training is the control and supervision of movement or flow of students through the training pipeline. A pipeline provides accountability and helps maintain the uninterrupted flow of students. Naval Education and Training (NAVEDTRA) Manual 135C, Chapter 3, Section 1, Paragraph 1.1.
[17] These systems include FLTMPS and TWMS.

DON Cyber/IT Workforce Strategic Plan for FY 2010-2013 provided overall CS/ITWF management-related responsibilities, but no specific training, certification, and development requirements. SECNAV Instruction 1543.2 establishes policy and procedures for DON's CS/ITWF professional development through a Continuous Learning Program to support the continuing professional development of the CS/ITWF and establishes related responsibilities. However, the instruction has no specific training, certification, and development requirements (see Exhibit A). Finally, as noted, five of eight criteria only pertained to the IAWF, so the instruction did not cover the entire CS/ITWF.

Table 1. Guidance for the Training, Certification, and/or Development of the CS/ITWF

Source	Purpose
SECNAV Instruction 3052.2, "Cyberspace Policy and Administration within the DON," dated 6 March 2009	Establishes policies and responsibilities for the administration of the CS/ITWF within DON.
SECNAV Instruction 1543.2, "Cyberspace/IT Workforce Continuous Learning," dated 30 November 2012	Establishes policy and procedures for DON CS/ITWF professional development through a Continuous Learning Program to support the continuing professional development of the CS/ITWF throughout their careers. The Continuous Learning Program will include education, training, certification, and other activities that support the sustainment and continued improvement of the capabilities of the DON CS/ITWF.
DON Cyber/IT Workforce Strategic Plan for FY 2010-2013	Establishes DON's priorities for ensuring workforce excellence. It identifies the goals and objectives that will allow DON to recruit, manage, develop, sustain, and retain a workforce engaged in network operations, information assurance, information management, information warfare, and computer network defense, as well as a workforce involved in the design, development, and implementation of IT national security, and business systems and programs.
DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," dated 23 April 2007	Establishes policy and assigns responsibilities for DoD Information Assurance training, certification, and workforce management.
DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Plan," dated 24 January 2012	Implements DoD Directive 8570.1 and provides guidance for the identification and categorization of positions and certification of personnel conducting Information Assurance functions within the DoD workforce supporting the DoD Global Information Grid (GIG).
SECNAV Instruction 5239.2, "DON Cybersecurity/Information Assurance Workforce Management, Oversight, and Compliance," dated 17 June 2010	Establishes policy and assigns responsibilities for the administration of the DON Cybersecurity/IAWF Management Oversight and Compliance Program.
SECNAV Instruction M-5239.2, "DON Information Assurance Workforce Management Manual," dated 29 May 2009	Describes DON IAWF management plans and establishes Information Assurance (IA) awareness requirements for information system users.
DON CIO Memo, "Guidance for Cybersecurity Workforce Operating System/Computing Environment Certification Compliance Process dated 8 February 2012"	Provides updated guidance for DON IAWF commercial operating system/computing environment certification requirements.

Training of CS/ITWF Personnel

The Navy did not provide sufficient training for CS/ITWF line officers or pipeline training for the IT/ITS ratings according to prescribed guidance.

CS/ITWF Line Officers. Although CS/ITWF line officers received the Information and Communications Manager Course (ICMC), the course provided only basic communications skills. Also, according to the officers' testimony and training documentation, they received no follow-on training to develop the technical skill sets needed to supervise the work of their CS/ITWF personnel. As a result, line officers told us they were heavily reliant upon their subordinate personnel and typically could not speak the technical language of the CS/ITWF personnel they supervised. Five of 20 line officers stated they did not have the appropriate skill sets to perform their current duties. According to the five officers' testimony, their proficiency and/or ability to carry out their assignments was also adversely affected by: under manning at the command; the temporary assignment of division personnel to duties outside their specialty (i.e., Security, Food Service Attendant, etc.); IT system owner limitations that prevented them from working on some systems (i.e., Navy Marine Corps Internet (NMCI), Space and Naval Warfare Systems Command, etc.); a heavy reliance upon civilian subject matter experts and Fleet Systems Engineering Teams,[18] and the lack of redundancies for critical people or equipment. Table 2 shows the results of our interviews with the CS/ITWF line officers regarding their IT skills and the state of IT at their ship or activity.

[18] The primary functions of the team are to keep the networks up and running, optimize the networks to meet changing mission requirements, and help ensure Command, Control, Communications, Computers, and Intelligence (C4I) end-to-end operability.

Table 2. Number of Officers Who Agreed the Following Conditions Existed for Them or at Their Afloat or Shore Activity

SUMMARY OF OFFICER CONDITIONS IDENTIFIED DURING SITE VISITS						
		Type of Afloat or Shore Activity				
	Conditions Identified	Naval Air Forces, Atlantic Carriers	Naval Surface Force, U.S. Atlantic Fleet Ships	Submarine Force Atlantic[19] Submarines	Shore Activities	TOTAL
	Number of Officers Interviewed	5	6	0	9	20
1	IT skill gaps exist at my ship or activity.	5	6		9	20
2	I am not working with primary Navy Officer Billet Codes (NOBC).	0	0		1	1
3	The IT function is under manned at my ship or activity.	3	6		6	15
4	Skill proficiency of officer IT personnel at my ship or activity is impacted by temporary assignment of IT personnel to non-IT functions.	3	2		3	8
5	Skill proficiency of officer IT personnel at my ship or activity is impacted by system owner limitations. (i.e., NMCI, Space and Naval Warfare Command (SPAWAR), or Vendor Warranty).	3	5		5	13
6	Skill proficiency of officer IT personnel at my ship or activity is impacted by reliance on Civilian Subject Matter Experts (SME), Fleet Systems Engineering Teams , and Tech Rep. workforce.	2	6		9	17
7	Training of officer IT personnel at my ship or activity is not obtained through alternative methods (On the Job Training (OJT), Personnel Qualification Standards (PQS), and cross-training).	0	1		0	1
8	I do not have appropriate skills to perform my CS/ITWF work roles.	0	3		2	5
9	A single point of failure exists at my ship or activity (i.e., no redundancies for critical people or equipment).	3	4		5	12

CS/ITWF Enlisted Personnel. Overall, personnel that we interviewed felt that they had sufficient skills to perform their daily tasks. However, personnel stated that they were provided training that was not relevant to their current tasks. They also stated that they received training geared more towards passing certification exams than supporting the Fleet. They further stated that they obtained minimal, if any, practical training experience. Therefore, they did not believe they had a full understanding of their roles and responsibilities. Furthermore, 30 of the 96 (31 percent) enlisted personnel interviewed stated that they did not have appropriate skills to perform their IT-related functions. These individuals believed they did not maintain a sufficient skill set to adequately perform their daily tasks and therefore, relied heavily upon their peers. Specifically, these individuals stated they were not provided formalized training for their current roles and thus lacked a fundamental understanding of their assigned areas. Some said they were required to work outside their Navy Enlisted Classification (NEC) and therefore, did not receive needed training. In some cases, the enlisted personnel said their proficiency and/or ability to carry out their assignments was also impacted by: under

[19] There were no CS/ITWF officers interviewed because none were detailed to the submarines visited for this audit.

manning, the temporary assignment of division personnel outside their rating, system owner limitations, the heavy reliance upon civilian subject matter experts and Fleet Systems Engineering Teams,[20] and the lack of redundancies for critical people or equipment.

Table 3. Number of Enlisted Personnel Who Agreed the Following Conditions Existed for Them or at Their Afloat or Shore Activity

SUMMARY OF ENLISTED CONDITIONS IDENTIFIED DURING SITE VISITS						
		Type of Afloat or Shore Activity				
	Conditions Identified	Naval Air Forces, Atlantic Carriers	Naval Surface Force, U.S. Atlantic Fleet Ships	Submarine Force Atlantic Submarines	Shore Activities	TOTAL
	Number of Enlisted Personnel Interviewed	15	31	10	40	96
1	IT skill gaps exist at my ship or activity.	11	22	10	25	68
2	I am not working with primary NEC	8	5	0	18	31
3	The IT function is under manned at my ship or activity.	6	24	9	17	56
4	Skill proficiency of enlisted IT personnel at my ship or activity is impacted by temporary assignment of IT personnel to non-IT functions.	9	19	8	14	50
5	Skill proficiency of enlisted IT personnel at my ship or activity is impacted by system owner limitations (i.e., NMCI , SPAWAR, or Vendor Warranty).	7	21	7	20	55
6	Skill proficiency of enlisted IT personnel at my ship or activity is impacted by reliance on Civilian Subject Matter Experts (SMEs), Fleet Systems Engineering Teams, and Tech Rep. workforce.	9	19	10	29	67
7	Training of enlisted IT personnel at my ship or activity is not obtained through alternative methods (OJT, PQS, and Cross-training).	1	0	3	0	4
8	I do not have appropriate skills to perform my CS/ITWF work roles.	6	11	3	10	30
9	A single point of failure exists at my ship or activity (i.e., no redundancies for critical people or equipment).	4	13	8	14	39

During our review of 116 CS/ITWF personnel, Navy Cyber Forces Command (type commander for training for CS/ITWF personnel) and activity personnel informed us that the training and career development they received was based on general billet positions and not on specific duties of IP Officer designators and the IT/ITS ratings. Further discussions with Navy Cyber Forces Command, OPNAV N2/N6, and DON CIO personnel confirmed that pipeline training and career development for IP Officer designators had not been developed. However, pipeline training and career development

[20] The primary functions of the team are to keep the networks up and running, optimize the networks to meet changing mission requirements, and help ensure Command, Control, Communications, Computers, and Intelligence (C4I) end-to-end operability.

for the IT/ITS ratings have been developed and are currently being revised, but have not been provided to all enlisted members in the IT/ITS ratings we interviewed.

Why Specific, Comprehensive Training Guidance Had Not Been Developed and CS/ITWF Personnel Were Not Sufficiently Trained

Responsible Navy personnel cited several reasons for (1) the lack of comprehensive training and certification guidance for the overall CS/ITWF (which includes active duty military members), and (2) insufficient active duty and enlisted member CS/ITWF training. The Navy placed a higher priority on the warfighters' needs and the development of the Information Assurance Workforce (IAWF) to comply with the Federal Information Security Management Act than on establishing the guidance or training necessary to provide career development for the entire CS/ITWF. Also, according to DON CIO personnel, the Navy was waiting for DoD to establish its overarching guidance in this area prior to issuing its own guidance.

However, SECNAV Instruction 3052.2, "Cyberspace Policy and Administration within DON," dated 6 March 2009, states that cyberspace operations require intensive training and education for the total DON Cyberspace Workforce to meet emerging technical developments. It also states that the CS/ITWF is critical for achieving DON objectives in every warfighting domain and enterprise business model. Also, OPNAV Instruction 1500.74A, "Utilization of Enlisted Occupational Standards for Training and Career Development," dated 26 January 2007, requires training and career development based on enlisted occupational standards, including formal schools, onboard training, on-the-job training, development of Personnel Advancement Requirements, and nonresident training packages (e.g., rate training manuals). For these reasons, as well as the potential impacts discussed in the finding, comprehensive training and certification guidance for the active duty military members of the overall CS/ITWF and sufficient active duty and enlisted member CS/ITWF training are needed.

Furthermore, training for CS/ITWF line officers was not sufficient. All line officers who we reviewed identified skill gaps. This occurred because the training currently available did not provide line officers with the skills needed to adequately supervise the work of the CS/ITWF personnel they supervised. For example, line officers were heavily reliant upon their subordinate personnel and typically could not speak the technical language of the CS/ITWF personnel they supervised. Five of 20 line officers stated they did not have the appropriate skill sets to perform their current duties. In some cases, the proficiency of the line officers and/or ability to carry out their assignments was also adversely affected by: under manning at the command, the temporary assignment of division personnel to duties outside their specialty (i.e., Security, Food Service Attendant, etc.), system owner limitations that prevented them from working on some systems (i.e., Navy Marine Corps Internet (NMCI), Space and Naval Warfare Systems Command, etc.), a heavy reliance upon civilian subject matter experts and Fleet Systems Engineering Teams, and the lack of redundancies for critical people or equipment.

Finally, concerning enlisted personnel, pipeline training for the IT/ITS ratings was not provided to all personnel. Naval Education and Training (NAVEDTRA) Manual 135c, Chapter 3, Section 1, Paragraph 1.1, states that pipeline training is the control and supervision of movement or flow of students through the training pipeline. A pipeline provides accountability and helps maintain the uninterrupted flow of students. According to the testimony of enlisted personnel, they believed that pipeline training for IT/ITS ratings would ensure that they have the skill sets needed, and they would be allocated to the appropriate IT/ITS work roles within DON throughout their Navy careers. Currently, the IT/ITS ratings have a broad spectrum of work roles and training (i.e., system administrators, radio communications, system security technicians, etc.), and personnel can be assigned to various work roles based on their IT/ITS rating and not necessarily on the training they received. In contrast, personnel in the Cryptologic Technician Network (CTN) rating are trained and assigned to duty stations based on training received within the training pipeline. DON CIO and OPNAV N2/N6 personnel agreed with enlisted personnel and the senior management we interviewed that pipeline training is needed for IT/ITS ratings.

Retention of CS/ITWF Training and Certification Documentation

Documentation to validate CS/ITWF training was not provided for 16 of the 116 officers and enlisted personnel reviewed. Documentation of training for the remaining 100 personnel was obtained from hard copies of documentation in the training jackets or from data found in FLTMPS or TWMS. For the commands audited, 100 of 116 active duty personnel provided 191 source documents (i.e., hard copies of training certificates) for CS/ITWF-related training completed. Although commands entered data from 122 of the CS/ITWF-related training documents into FLTMPS, they did not enter information for 69 source documents. In addition, although commands entered data from 123 of the CS/ITWF-related training documents into TWMS, they did not enter data for 68 source documents. See Table 4 for a summary of training records requested and received, including the source of the training documentation provided.

Table 4. Retention of CS/ITWF Training and Certification Documentation

Selected Activities	ENLISTED PERSONNEL INTERVIEWED					OFFICERS INTERVIEWED					Total # of Training Records Received ***
	#	# Training Record Received	Source of Training Records			#	# Training Record Received	Source of Training Records			
			Source Documents Received**	Not Recorded in FLTMPS*	Not Recorded in TWMS			Source Documents Received**	Not Recorded in FLTMPS*	Not Recorded in TWMS	
Afloat Activities											
USS George H.W. Bush	8	8	5	5	0	2	1	1	0	0	6
USS Theodore Roosevelt	7	7	16	5	0	3	3	3	1	0	19
USS Cole	8	8	0	0	0	2	2	0	0	0	0
USS Boise (SSN 764)	1	1	0	0	0	0	0	0	0	0	0
USS Montpelier SSN 765)	3	3	0	0	0	0	0	0	0	0	0
USS Newport News (SSN 750)	2	2	0	0	0	0	0	0	0	0	0
USS Scranton (SSN 756)	4	4	0	0	0	0	0	0	0	0	0
USS Vella Gulf	6	5	6	6	6	4	3	4	4	4	10
USS Elrod	7	6	32	6	30	0	0	0	0	0	32
USS Bulkeley	10	1	8	0	0	0	0	0	0	0	8
Afloat Activity Total	**56**	**45**	**67**	**22**	**36**	**11**	**9**	**8**	**5**	**4**	**75**
Ashore Commands											
Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT)	7	7	0	0	0	3	3	0	0	0	0
Navy Cyber Defense Operations Command (NCDOC)	8	8	40	29	17	2	2	10	8	6	50
Navy Cyber Forces Command	8	8	26	4	2	2	2	0	0	0	26
Space and Naval Warfare Command Tidewater	9	6	21	0	3	1	0	0	0	0	21
Space and Naval Warfare Command Space Field Activity Chantilly	8	7	18	1	0	1	1	1	0	0	19
Ashore Activity Total	**40**	**36**	**105**	**34**	**22**	**9**	**8**	**11**	**8**	**6**	**116**
Total (Afloat and Ashore)	**96**	**81**	**172**	**56**	**58**	**20**	**17**	**19**	**13**	**10**	**191**

*Total FLTMPS training records provided = 122 [191 - (56 +13)].
**Total number of active duty personnel who provided source documents = 100 (81 Enlisted +19 Officers).
***Total number of personnel that did not provide any training and certification documentation = 16 (116-100).

The training records were not available because internal controls were not in place to ensure that CS/ITWF-related training records were maintained and readily available. Further, internal controls were not in place to ensure that training completed by CS/ITWF personnel reviewed at the selected commands was recorded in FLTMPS or TWMS.[21] In addition, although FLTMPS and TWMS include some training data, the Navy does not have a database to capture all training. Afloat command personnel explained there are various systems used to record training. For example, afloat and ashore commands may input training data into systems such as FLTMPS or TWMS. We found instances where active duty personnel completed CS/ITWF-related training prior to arriving at their current duty station, and the training was not recorded in FLTMPS and TWMS. In these instances, the receiving command (command visited during the audit) could not provide source documents (i.e., electronic or hard copies of training certificates). As a result, we requested source documents from personnel we reviewed and found that as noted, not all personnel maintained supporting documents for training. We determined that: various systems were used to record training data; the most commonly used systems (FLTMPS or TWMS) did not accurately reflect all training records; and of the available systems, none documented all training received by CS/ITWF personnel. As result, we could not rely on the commands audited to provide complete training records for their personnel and instead had to obtain training records from multiple systems and rely on reviewed personnel to provide source documents when available.

Impact

Lack of training and certification guidance, and insufficient officer and enlisted CS/ITWF training may impact fleet and shore activity readiness. Line officers may lack the ability to oversee CS/ITWF-related staff, and the number of available active duty personnel with the technological skill sets needed for Cyberspace/IT work roles may be limited. Without a centralized, comprehensive training/certification records system for CS/ITWF, Navy commands cannot accurately determine personnel proficiency and skill gaps. Navy commands cannot use the workforce in the most efficient and effective manner, nor can they establish and track training, manpower, and continuing education requirements as required.

[21] FLTMPS and TWMS are two systems that maintain electronic records showing training completed and certifications earned for active duty military members.

Recommendations

We recommend that the Department of the Navy Chief Information Officer:

Recommendation 4. Develop and issue training and certification guidance for the overall Cyberspace/Information Technology Workforce. At a minimum, this guidance should:

- Identify the specific ratings, occupational codes, and work roles that comprise the overall Cyberspace/Information Technology Workforce to ensure even the most junior members of the Cybersecurity and remaining Cyberspace/ Information Technology Workforce understand they comprise the overall Cyberspace/Information Technology Workforce.

- Clearly state procedures for the training, certification, and management of the entire Department of the Navy Cyberspace/Information Technology Workforce.

- Require that this guidance be communicated to all levels within the Department of the Navy.

Department of the Navy Chief Information Officer response to Recommendation 4. Concur. Also, see Department of the Navy Chief Information Officer (DON CIO) response to Recommendation 1. DON CIO is working with the Department of Defense (DoD), Navy, and Marine Corps to update current guidance and procedures. This includes addressing revisions to DoD and DON Information Assurance Workforce policy. The planned release for the guidance is 30 September 2014.

Naval Audit Service comments on response to Recommendation 4. Actions planned by management meet the intent of the recommendation. A 29 April 2014 DON CIO e-mail provided clarification to the management response. The e-mail stated that the soon to be signed out DoD guidance shows that the Cyberspace Workforce includes the cyberspace information technology and Cybersecurity Workforces (the e-mail provided definitions of each workforce). It further stated that DON CIO, Navy, and the Marine Corps are currently validating all positions within DON that are within the Cyberspace Workforce in the categories of Cybersecurity and Cyberspace/Information Technology (IT). Cyberspace/IT is not the current high-level term for the overall Cyberspace workforce. As a part of this effort, every position will be coded with an Office of Personnel and Management-approved "Cybersecurity Code." Cybersecurity is the term agreed upon at the

national level for what DoD calls the Cyberspace Workforce. This code applies to specialty areas within the National Initiative for Cybersecurity Education framework as configured for DON use. DON will identify training, education, certification, and qualification requirements for each specialty area that encompasses the Cybersecurity and Cyberspace/IT specialty areas. The recommendation is considered open pending completion of agreed-to actions.

We recommend that the Deputy Chief of Naval Operations (Information Dominance) (OPNAV N2/N6) [22]:

Recommendation 5. Redefine training requirements for Cyberspace/Information Technology Workforce line officers to ensure that they have the education and competencies needed to support the Department of the Navy's mission, goals, and dynamic workforce structure changes. Also, ensure that Cyberspace/Information Technology Workforce line officers can provide proper oversight over the enlisted Cyberspace/Information Technology Workforce.

Deputy Chief of Naval Operations (Information Dominance) (OPNAV N2/N6) response to Recommendation 5. Concur. OPNAV N2/N6 recently approved Program Objective Memorandum (POM) resources that will restructure and provide timely technical updates and significantly increase the "time to train" for Information Professional (IP) officers attending the IP Basic course. Currently the course is optional for new IP officers and is only 4 weeks in length. However, approved funding actions have increased the length of the course from 4 to 8 weeks and will be "mandatory" for all new accession IP officers. The timeline for implementing the new course is Fiscal Year (FY) 2016. N2/N6 is also reviewing strategies to integrate aspects of IT enlisted technical training into the IP officer pipeline for added robustness. N2/N6 is conducting internal reviews to identify student resources that would allow expanded numbers of IP officers to attend the Marine Corps' C4I Officer Community of Interest (COI) (26 weeks). The Marine Corps course is expeditionary-focused and closely parallels the technical responsibilities of an IP officer. The issue of non-IP officers serving in the Cybersecurity workforce management roles is an ongoing discussion being coordinated with the United States Fleet Forces Command, N2/N6, the ID Type Commander and other community leadership. Although N2/N6 recognizes that the current organizational construct is not optimal for non-IP officers managing Cybersecurity workforce requirements, the "way-ahead" decision will be determined at Echelon 1 in coordination with the respective Fleet and Type

[22] The OPNAV N2/N6 response to Finding 2 stated that for purposes of clarity, any N2/N6 response on CSWF in this document (pertaining particularly to responses to Recommendations 5 and 7-9) refers only to Cybersecurity Workforce personnel within the Cyberspace Workforce Program. Once the Cyberspace Workforce is clearly defined by DoD and DON CIO, OPNAV N2/N6 will ensure appropriate workforce alignment of applicable roles and responsibilities.

Commanders. However, until a final determination is made, the N2/N6 Cybersecurity workforce mitigation strategy will be: (1) Provide clear and unambiguous Echelon 1 Cybersecurity workforce policy guidance to all levels of the Navy enterprise; (2) Provide commanding officers with the most knowledgeable, technically proficient and operationally sound cadre of senior enlisted IT leadership possible that will assist in the oversight and management of command cyberspace/IT workforce requirements.

In reference to changes to the IP Officer course, the expected date of implementation is May 2016. For the more immediate mitigation efforts, N2/N6 responses are predicated on DON CIO's update to Secretary of the Navy (SECNAV) Instruction 5239 along with the release of the DoDD 8140.aa. Once these documents have been promulgated (estimated date of completion in September 2014), OPNAV N2/N6 will release a Naval Administrative Message (NAVADMIN) that will direct the fleet to these changes and ensure implementation of all directives and instructions. Estimated release date for the NAVADMIN will be May 2015.

Naval Audit Service comments on responses to Recommendation 5. Planned actions meet the intent of the recommendation. The recommendation is considered open pending completion of agreed-to actions.

Recommendation 6. Ensure Information Systems Technician/Information Systems Technician (Subsurface) Cyberspace/Information Technology Workforce enlisted personnel have pipeline training and career development reflecting current set of competencies and skills needed to perform Cyberspace/Information Technology Workforce work roles.

Deputy Chief of Naval Operations (OPNAV N2/N6) response to Recommendation 6. Concur. The Information System Technician (Surface/Subsurface) ratings have established training pipelines that support all new Information Systems Technician/Information Systems Technician (Subsurface) (IT/ITS) accession requirements and the required disciplines to operate in the Cyber domain. Although the IT rating is managed more as a generalized community of IT technical personnel, there is ongoing Flag dialogue to consider measures that potentially could restructure and reconstitute the rating. This new structure, in theory, would require specific personnel or ratings to perform independently focused/specialized IT functions using either "Core/Strand" architecture or as independently managed communities (ratings). However, because of the pervasiveness of Internet Protocol (IP) technology and the inevitability of EOIP (Everything over Internet Protocol), all personnel would be expected to be trained on the basics of IP technology. Upon graduation, these personnel would then either specialize Navy Enlisted Classification Codes (NEC)

or be integrated into separate and distinct ratings solely responsible for either Radio Frequency (RF) Communications, Internet Protocol (IP) Networking/System Administration, Computer Network Defense, Technical Control, Communications Administration, System Maintenance, etc. This effort is ongoing and is under review by the Navy Information Dominance (IDC) Flag Panel.

The ITS rating is responsible for managing Internet Protocol (IP)-based functions within the submarine Networks/Communications architecture. The Electronics Technician-Communications (ETR) rating (sub communications) personnel perform RF/Baseband functions aboard submarines that would be typically performed by IT (surface) personnel. Both ratings (IT/ITS) are designated as Advanced Technical Fields and attend the initial 19 weeks of 'A' School at the Center for Information Dominance (CID) in Corry Station. Upon graduation, select IT/ITS personnel are identified to receive follow-on NEC producing 'C' Schools and additional training/certifications before going on to the fleet.

The ITS rating was stood up in 2010 to address the unique Cyber IT requirements of the submarine Local Area Network (LAN) functions only. This requirement was previously managed by various submarine ratings (Fire Control Technicians (FT)/ Electronics Technicians (ET)/ Sonar Technician, Submarine (STS)) but impaired those ratings' ability to perform their normal rating functions. To ensure proper growth and development, the IT/ITS ratings are managed by a respective OPNAV Enlisted Community Manager (ECM) responsible for the required training and career development across the entire community covering a 20 year career.

Whether IT personnel become more specialized or not, they are always at the cutting edge of new technology advancements and were targeted to participate in a recently completed 2-year Defense Advanced Research Projects Agency (DARPA) research project to identify and assess the significance of Artificial Intelligence in a Learning Environment. DARPA, OPNAV N1, and N2/N6 funded the concept, which is designed to significantly increase the knowledge/technical level (Six Sigma gain) of randomly selected Information Systems Technician (IT) students. This DARPA project developed an Intelligent Tutor that achieved its stated goals and received personal acknowledgement from the Chief of Naval Operations (CNO) for N2/N6 to implement this training technology into the IT 'A' school as soon as possible. The Navy is actively working with industry to acquire this Intelligent Tutor capability. Once a commercial service contract is signed with Navy, new accession students could begin training in this new technology as early as October 2014.

The identified IDC Flag Panel, which is reviewing future plans for the Information Systems Technician Rating, is expected to decide on a course of action by October 2014. The date for implementation of the DARPA/Intelligent Tutor training in the IT 'A' school is dependent upon the commercial service contract, which is scheduled to be completed by October 2014. Students will begin training by January 2015.

Naval Audit Service comments on responses to Recommendation 6. Planned actions meet the intent of the recommendation. The recommendation is considered open pending completion of agreed-to actions. A 14 May 2014 OPNAV N2/N6 e-mail supplementing their response stated that the NAVADMIN cited in earlier responses will include guidance that will address those activities that continue to assign personnel to Cybersecurity Workforce positions that do not hold the requisite DoD/OPNAV training/certifications. This guidance will be predicated on updated Secretary of the Navy guidance, and it will reiterate/reemphasize DoD policy that requires only properly trained/certified personnel are assigned to Cybersecurity Workforce positions. Properly trained/certified Cybersecurity Workforce personnel are reportable inspection items conducted by Command Cyber Readiness Inspections (CCRI). We note that per the response to Recommendation 5, estimated release date for the NAVADMIN message will be May 2015.

Recommendation 7. Establish a centralized system to track and maintain a complete training history for Cyberspace/Information Technology Workforce personnel. This system should ensure that all source data systems which maintain electronic training and certification records are readily identifiable, and that training and certification records are maintained in cases for which records are not recorded on other systems.

Deputy Chief of Naval Operations (OPNAV N2/N6) response to Recommendation 7. Concur. Since the initial date of this audit, Navy has made significant strides in how it identifies, manages, trains, and tracks Cybersecurity Workforce personnel. Further, SECNAV Instruction 5239 facilitates Navy internal Cybersecurity Workforce management standards. The Total Workforce Management System (TWMS) is currently identified as the Navy's primary enterprise data system of choice as previously cited in the DON CIO response to Recommendation 3. However, the iterative Echelon 1 and Functional Area Manager (FAM) process known as Application and Rationalization (APPRAT) will address the continued usability, supportability, and any duplication of effort concerns between TWMS and other approved workforce management Programs of Record (POR) for purposes of long-term sustainability. In the interim, TWMS will be used as the enterprise management tool for capturing required Cybersecurity Workforce data. Ongoing improvements are being made to the system to remove any known gaps or system shortcomings.

In a parallel, but unrelated, effort and at the direction of the Chief of Naval Operations (CNO), OPNAV N2/N6 instituted the first ever Cyber Integrated Readiness Assessment (IRA), which identifies the current and future readiness posture of a specific Warfare Domain (Cyber). The IRA is influenced by data pulled from the Defense Readiness Reporting System Navy (DRRS-N) and mandates unit reporting on specific command readiness attributes known as Readiness Pillars. Operational units report the status of their Personnel, Equipment, Supply, Training, and Ordinance (PESTO) pillars semi-annually to CNO via the IRA. Although initial IRA analysis of the Cyber Domain identified that not all activities are reporting all aspects of their cyber posture, it is expected that succeeding iterations of this DRRS-N process will help facilitate 100 percent reporting and compliance. The Cyber (Assured C2) IRA is expected to be an excellent adjunct reporting tool in support of Cybersecurity Workforce posture and TWMS. Upon further review and approval by OPNAV N2/N6 Flag leadership, a NAVADMIN message will be released to the fleet that will address the current ambiguity surrounding the Cybersecurity Workforce and reinforce the applicability of SECNAV Instruction 5239 requirements across the Navy enterprise.

DON CIO's release of the updated Secretary of the Navy Instruction will detail the extent that TWMS will be utilized as a tracker of the Cyberspace workforce. Following that release as mentioned under Recommendation 5 will be the N2/N6 NAVADMIN detailing the requirements to fully populate TWMS with all Cybersecurity Workforce personnel. There is an expected goal date of May 2015.

Naval Audit Service comments on responses to Recommendation 7. Planned actions meet the intent of the recommendation. The recommendation is considered open pending completion of agreed-to actions. A 14 May 2014 OPNAV N2/N6 e-mail supplementing their response stated that TWMS is being expanded to capture all required National Institute of Standards and Technology framework data fields and will provide a central source for tracking all Cybersecurity Workforce personnel along with their complete training history. Updates are ongoing. The system, per DON CIO guidance, is expected to be fully functional by 1 October 2014.

Recommendation 8. Establish procedures and related internal controls requiring that electronic or hard copy training records and certifications be retained for all Cyberspace/Information Technology Workforce active duty military members as required by SECNAV Manual M-5210.1, "Department of the Navy Records Management Program, Records Management Manual."

Deputy Chief of Naval Operations (OPNAV N2/N6) response to Recommendation 8. Concur. Per the requirements as cited in DoD Instruction 8570.1 and SECNAV Instruction 5239, N2/N6 is actively coordinating with DON CIO, Fleet Cyber Command/10th Fleet, the newly established Information Dominance TYCOM (Navy Cyber Forces Command), and Fleet TYCOMs in order to ensure the required internal controls are understood and properly documented by all stakeholders. We are also reviewing applicable Air, Surface, Subsurface, and Expeditionary Force Readiness Training Manuals. Furthermore, we are looking at the applicability of the Cybersecurity Inspection Program (CSICP) and Command Cyber Readiness Inspections (CCRI) to ensure unit network security management and "inspection ready" criteria for the Cybersecurity Workforce is properly understood, in place, and reported. N2/N6 is also reviewing the Information System Security Manager (IT 2779) Information Assurance Manager (IAM) course of instruction for applicability to activity level enforcement of Manager's Internal Control Program (MICP) requirements. These actions (in conjunction with the IRA, release of the previously mentioned NAVADMIN, annual General Military Training (GMT), etc.) will ensure that all unit Commanding Officers (COs), Command Information Assurance Managers (IAM), and crew and individual Cybersecurity Workforce personnel are aware and knowledgeable of the SECNAV MICP 5200 checklist and administrative requirements to document and track Cyberspace/Information Technology Workforce personnel.

This recommendation will also be using the previously mentioned NAVADMIN, with a goal release date of May 2015.

Naval Audit Service comments on responses to Recommendation 8. Planned actions meet the intent of the recommendation. The recommendation is considered open pending completion of agreed-to actions.

Recommendation 9. Until the centralized system is established as recommended in Recommendation 7, establish procedures and related internal controls requiring that all Cyberspace/Information Technology Workforce training records and certifications be recorded/entered into the Fleet Training Management and Planning System or Total Workforce Management System as required.

Deputy Chief of Naval Operations (OPNAV N2/N6) response to Recommendation 9. Concur. TWMS is the interim enterprise management tool that Navy will use for identifying, tracking, and managing Cybersecurity Workforce personnel. As previously stated, the iterative Echelon 1 and Functional Area Manager (FAM) process known as Application and Rationalization (APPRAT) will address any usability, supportability, or duplication of effort concerns that might exist between TWMS and other approved workforce

management Programs of Record (POR) in terms of long term viability and sustainability.

Further review of existing policy and discussions with DON CIO indicates additional SECNAV policy is forthcoming to address the internal controls management requirement for Cybersecurity Workforce personnel. In the interim, N2/N6 intends to address this issue in the NAVADMIN (pending Flag approval) that will speak to the specifics and identification of Cybersecurity Workforce personnel, required management policy, procedures, and training requirements as identified in the prior responses. As an additional data metric, N2/N6 also intends to track the reporting of Cybersecurity Workforce management requirements by individual unit reporting via DRRS-N and the applicable Cyber IRA. N2/N6 is also reviewing this requirement with the CID Learning Center to ensure it is being addressed sufficiently in the Information Systems Security Managers course that trains Information Assurance Managers (IAMs).

This recommendation will be utilizing the before mentioned NAVADMIN with a goal release date of May 2015. In addition, the Information Systems Security Managers course review will take place by November 2014, and corrections or addition of the training topics of the Cybersecurity Workforce in totality will include documenting, tracking and record management of the work force.

Naval Audit Service comments on responses to Recommendation 9. Planned actions meet the intent of the recommendation. The recommendation is considered open pending completion of agreed-to actions.

Finding 3: Department of the Navy Managers' Internal Control Program

Synopsis

Fourteen of 15 activities we reviewed did not include the CS/ITWF in their assessable units for the FY 2013 Managers' Internal Control Program (MICP) at the activity or higher command levels. According to SECNAV Instruction 5200.35E, "Department of the Navy (DON) Managers' Internal Control Program (MICP)," management is required to maintain a list of assessable units covering the entire organization at the activity or higher levels; and to evaluate and document internal control evaluations for these assessable units using existing sources of data or separate internal control evaluations if existing data is not adequate. This condition occurred because:

- Managers on U.S. Fleet Forces Command ships were not aware of the MICP;
- U.S. Fleet Forces Command MICP coordinators relied on ship/submarine Inspections, Certifications, Assessments and Visits (ICAVs) to satisfy MICP internal control evaluation requirements with no supporting documentation or supporting assessable unit to show specifically that internal controls were evaluated in accordance with MICP requirements in the CS/ITWF area; and
- Of a lack of Navy MICP guidance specifically concerning the CS/ITWF and use of commanders' discretion as to what specific areas of their organization to assess.

In our opinion, since CS/ITWF is not included in assessable units in command MICPs, there is no assurance that internal controls are evaluated in this area or material weaknesses are noted and reported to higher levels. This can lead to the ineffective use of limited resources (both personnel and funds). The lack of documented oversight can have an impact on mission readiness.

Discussion of Details

Background

Inspections, Certifications, Assessments and Visits (ICAVs). ICAVs are used within the U.S. Fleet Forces Command to evaluate mission performance. ICAVs are used to (1) inspect operational proficiency and identify material conditions; (2) ensure equipment and systems, including personnel/organizations needed to properly employ the equipment and systems, are certified as required; and (3) assess key systems, processes and results of an organization using an established framework and methodology.

Pertinent Guidance

SECNAV Instruction 5200.35E, "DON Managers' Internal Control Program (MICP)," dated 8 November 2006, provides guidance to implement Federal Managers' Financial Integrity Act (FMFIA) requirements within the Navy. The instruction requires that assessable units, DON Major Assessable Units, and their immediate subordinate commands establish, evaluate, and improve internal controls and oversee the performance of risk assessments within their organizations. This instruction requires that activities assign MICP coordinators who are required to ensure that periodic internal control evaluations for assessable units are documented.[23] Inventories of assessable units that constitute the entire organization (meaning every part of the organization must be represented) are required. The assessable unit must be large enough to detect any weakness that could impact the organization's mission, but small enough to allow the manager to perform a meaningful evaluation of internal controls.

SECNAV Manual 5200.35, "DON Managers' Internal Control Manual," dated 2 June 2008, states that management is to maintain a list of assessable units, with purpose and objective, and should use this list when planning any system review of internal controls.

OPNAV Note 5200, "FY 2013 MICP Reporting Requirements," dated 7 May 2013, states that all Navy commands are responsible for assessing whether adequate internal controls are in place and operating effectively.[24]

Audit Results

Fourteen of 15 activities we reviewed did not include CS/ITWF in their assessable units for the FY 2013 MICPs at the activity or higher command levels.

MICP Inclusion

[23] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," dated 30 May 2013, which SECNAV Instruction 5200.35E implements (SECNAV Instruction 5200.35E, dated 8 November 2006, page 1, reference (d)), states on page 11, paragraph 6 that DoD components must "assess the effectiveness of internal controls through a process consistent with Managers' Internal Control Program guidance. This process must include risk assessments, the identification of internal controls, and internal control testing. Leverage any and all existing management assessments, evaluations, continuous process improvement project results, established 'best practices,' and recent audit findings, if applicable. Recent audit findings must not be the primary support of an assessable unit's evaluation of [internal controls] and must only be used to further substantiate management's conclusions. Identify internal control deficiencies primarily through testing conducted by the assessable unit manager at the assessable unit level. Other sources of information such as audits, inspections, investigations, management assessments, and credible information of nongovernmental origin may also identify an internal control deficiency."

[24] We found that the three Echelon II commands we reviewed (U.S. Fleet Forces Command, U.S. Fleet Cyber Command, and Space and Naval Warfare Systems Command) submit MIC certification statements to the Office of the Chief of Naval Operations. These commands, in turn, require subordinate activities to submit Managers' Internal Control (MIC) certification statements to them. The overall MIC certification statement is primarily developed from the individual submissions from the Type Commanders (TYCOMs)/Immediate Superior in Commands (ISIC), who gather documentation from their subordinate commands. The ISICs submit required documentation to the Echelon II Command MICP coordinator.

We reviewed 15 activities under three Echelon II commands (Finding 2 shows universe and sample selection methodology for the 15 activities) as shown in Table 5.

Table 5. Sites Visited and Related Echelon II and III Commands

Sites Visited	Echelon III Command (ISIC)[25]	Echelon II Command
2 Carriers	**Naval Air Forces, Atlantic**	**U.S. Fleet Forces Command (10 afloat activities/1 shore activity)**
4 Ships	**Naval Surface Force, Atlantic**	
4 Submarines	**Naval Submarine Force, Atlantic**	
Navy Cyber Forces Command		
Navy Cyber Defense Operations Command		**U.S. Fleet Cyber Command (2 shore activities)**
Naval Computer and Telecommunications Area Master Station, Atlantic		
Space and Naval Warfare Systems Command Space Field Activity		**Space and Naval Warfare Systems Command (2 shore activities)**
Space and Naval Warfare Systems Center Atlantic		

To determine if CS/ITWF was included in assessable units, we interviewed management personnel for each of the ships and submarines we visited, as well as at Echelon III command levels (Immediate Superiors in Command (ISICs) for ships and submarines reviewed). We also interviewed MICP coordinators at each of the shore activities visited. Additionally, we obtained supporting assessable unit listings. We did this to determine if:

- Ship managers were aware of the MICP;
- Assessable units included CS/ITWF; and
- Management control evaluations were performed for CS/ITWF.

Only Space and Naval Warfare Systems Center Atlantic included CS/ITWF in its inventory of assessable units. Additionally, the 14 activities that did not include the overall CS/ITWF as an assessable unit listed cybersecurity/information assurance as an assessable unit.

Why Conditions Occurred

U.S. Fleet Forces Command: Ships/Submarines. Managers at the ships who we interviewed said they were not aware of the MICP. MICP coordinators for ISICs responsible for these ships and submarines informed us that they believe they are not

[25] Immediate Superiors in Command (ISICs) for the ships and submarines.

required to push MICP requirements down to the ship and submarine level. However, the MICP requires management involvement at all levels in establishing, evaluating, and improving internal controls.

Further, the ISIC MICP coordinators informed us that ship/submarine ICAVs assessed readiness for the ships and submarines and that they believed it did not make sense to require additional assessments for the MICP. However, no assessable units were available for the overall CS/ITWF at any level. Also, management provided no documentation to show that ICAVs assessed internal controls for any aspect of the CS/ITWF area.[26] Including a specific assessable unit in the MICP at the Echelon II or ISIC level for CS/ITWF would show how ICAVs assessed these controls, and if not, support the need for a separate assessment of CS/ITWF-related internal controls per MICP requirements. As noted previously, (1) assessable units must cover the entire organization, and (2) internal controls for assessable units should be evaluated, whether existing sources of data are used or not, and (3) internal control evaluations must be documented.

Finally, we reviewed ISIC-level assessable units to determine whether they included the cybersecurity/information assurance portion of the overall CS/ITWF workforce. All 3 ISICs responsible for the 10 ships and submarines reviewed included the cybersecurity/information assurance portion. However, as noted earlier, a review of the entire CS/ITWF as an assessable unit would provide more coverage than just a review of the cybersecurity/information assurance portion of the CS/ITWF.

U.S. Fleet Forces Command: Navy Cyber Forces Command. This command was using the U.S. Fleet Forces Command list of assessable units. They stated that they planned to add the Cybersecurity Workforce portion of the CS/ITWF for FY 2014. However, they said that although SECNAV Instruction 5200.35E states management is required to maintain a list of assessable units covering the entire organization, it is also left to commander's discretion as to what areas they believe need to be assessed.

U.S. Fleet Cyber Command. Navy Cyber Defense Operations Command and Naval Computer and Telecommunications Area Master Station Atlantic included the cybersecurity/information assurance portion of the overall CS/ITWF workforce in their assessable units, but not the overall CS/ITWF, due to lack of Navy MICP guidance specifically concerning the CS/ITWF. Both activities said they plan to include the CS/ITWF as an assessable unit for FY 2014.

Space and Naval Warfare Systems Command. Space and Naval Warfare Systems Center Atlantic included Cyber and Influence Warfare and several other IT-related

[26] Navy Cyber Command provided ICAV inspection procedures for the U.S. Fleet Forces Command for the information assurance portion of the CS/ITWF. Commander, Submarine Force Atlantic provided corresponding ICAV inspection procedures for submarines. However, commands did not provide documentation of inspections made under these procedures, and no corresponding procedures were available for the remainder of the overall CS/ITWF.

assessable units, which we concluded covered the CS/ITWF sufficiently. Space and Naval Warfare Systems Command Space Field Activity included the cybersecurity/information assurance portion of the overall CS/ITWF workforce in its assessable units, but not the overall CS/ITWF, due to lack of Navy MICP guidance specifically concerning the CS/ITWF. The activity said it plans to include the CS/ITWF as an assessable unit for FY 2014.

Impact
In our opinion, since CS/ITWF is not included in assessable units in command MICPs, there is no assurance that internal controls are evaluated in this area or material weaknesses are noted and reported to higher levels. This can lead to the ineffective use of limited resources (both personnel and funds). The lack of documented oversight can have an impact on mission readiness. Finding 2 shows the potential impacts at the activity level of not having sufficient internal controls to ensure that CS/ITWF personnel have the proper skill sets.

Recommendations

We recommend that the Department of the Navy Chief Information Officer:

Recommendation 10. Require that all Navy commands with Cyberspace/Information Technology Work Force personnel include the Cyberspace/Information Technology Work Force in their assessable units for the Managers' Internal Control Programs and perform and document internal control evaluations for these assessable units using existing sources or separate evaluations, as required.

Department of the Navy Chief Information Officer response to Recommendation 10. Concur. Guidance will be included in the revision of Secretary of the Navy (SECNAV) Manual 5239.2, DON [Department of the Navy] Information Assurance Workforce Management Manual. This manual is being updated as the "Cybersecurity Workforce Management Manual." The planned release for this guidance is 30 September 2014.

Naval Audit Service comments on response to Recommendation 10. Actions planned by management to revise SECNAV Manual 5239 for the Cybersecurity Workforce meet the intent of the recommendation. A 29 April 2014 DON Chief Information Officer (DON CIO) e-mail provided clarification to the management response (see Recommendation 4) on the applicability of the response to the Cyberspace/Information Technology Workforce. The e-mail stated that soon to be signed out Department of Defense (DoD) guidance shows that the Cyberspace Workforce includes the Cyberspace Information Technology and Cybersecurity Workforces (the e-mail provided

definitions of each workforce). It further stated that DON CIO, Navy, and Marine Corps are currently validating all positions within DON that are within the Cyberspace Workforce in the categories of Cybersecurity and Cyberspace IT and that Cyberspace/IT is not the current high-level term (for the overall Cyberspace workforce). As a part of this effort every position will be coded with an Office of Personnel and Management-approved "Cybersecurity Code." Cybersecurity is the term agreed upon at the national level for what DoD calls the Cyberspace workforce.

Additionally, a 30 April 2014 DON CIO e-mail clarifying the management response further stated that they will address all recommendations. The problem, they stated, was that the Naval Audit Service used the term "Cyberspace/IT Workforce," which they say is no longer the proper term. Concerning the DoD Cyberspace and the DON Cybersecurity frameworks, they noted that the categories and specialty areas in the DON model address all of the areas that cover Cybersecurity and Information Technology. Further, the manual (cited in the response to Recommendation 10) has sections for compliance and assessment, and the cornerstone for those sections is the Manager's Internal Control Program. As noted above, the term, Cybersecurity Workforce, is being used at the national level to reflect the overall Cyberspace Workforce and includes the Cyberspace/Information Technology Workforce. The recommendation is considered open pending completion of agreed-to actions.

Recommendation 11. Ensure that management at all afloat activities are aware of their responsibilities for establishing, evaluating, and improving internal controls for the Cyberspace/Information Technology Workforce under the Managers' Internal Control Program.

Department of the Navy Chief Information Office response to Recommendation 11. Concur. Guidance will be included in the revision of SECNAV Manual 5239.2, DON Information Assurance Workforce Management Manual. This manual is being updated as the "Cybersecurity Workforce Management Manual." The planned release for this guidance is 30 September 2014. DON CIO e-mails from 29 and 30 April 2014, clarifying the Recommendation 10 response as to the applicability of the response to the Cyberspace/Information Technology Workforce, also applies to Recommendation 11.

Naval Audit Service comments on response to Recommendation 11. Actions planned by management to revise SECNAV Manual 5239 for the Cybersecurity Workforce meet the intent of the recommendation.

As noted above, the term Cybersecurity Workforce is being used at the national level and includes the Cyberspace/Information Technology Workforce. The recommendation is considered open pending completion of agreed-to actions.

Section B:

Status of Recommendations

Recommendations							
Finding[27]	Rec. No.	Page No.	Subject	Status[28]	Action Command	Target or Actual Completion Date	Interim Target Completion Date[29]
1	1	14	Develop and issue guidance to convey to the members of the DON Cyberspace/Information Technology Workforce their inclusion and role within the Cyberspace/Information Technology Workforce structure. At a minimum, this guidance should: • Include all necessary information to ensure even the most junior personnel of the Cybersecurity and remaining Cyberspace/Information Technology Workforce understand that they comprise the overall Cyberspace/Information Technology Workforce. • Require that this guidance be communicated to all levels within the Department of the Navy.	O	Department of the Navy Chief Information Officer	9/30/2014	
1	2	15	Establish workforce requirements to identify and track positions, personnel, and qualifications within the Cyberspace/Information Technology Workforce.	O	Department of the Navy Chief Information Officer	9/30/2014	
1	3	15	Establish workforce requirements to identify and track positions, personnel, and qualifications within the Cyberspace/Information Technology Workforce.	O	Department of the Navy Chief Information Officer	12/31/2014	

[27] / + = Indicates repeat finding.
[28] / O = Recommendation is open with agreed-to corrective actions; C = Recommendation is closed with all action completed; U = Recommendation is undecided with resolution efforts in progress.
[29] If applicable.

Recommendations							
Finding[27]	Rec. No.	Page No.	Subject	Status[28]	Action Command	Target or Actual Completion Date	Interim Target Completion Date[29]
2	4	31	Develop and issue training and certification guidance for the overall Cyberspace/Information Technology Workforce. At a minimum, this guidance should: • Identify the specific ratings, occupational codes, and work roles that comprise the overall Cyberspace/Information Technology Workforce to ensure even the most junior members of the Cybersecurity and remaining Cyberspace/ Information Technology Workforce understand they comprise the overall Cyberspace/Information Technology Workforce. • Clearly state procedures for the training, certification, and management of the entire Department of the Navy Cyberspace/Information Technology Workforce. • Require that this guidance be communicated to all levels within the Department of the Navy.	O	Department of the Navy Chief Information Officer	9/30/2014	
2	5	32	Redefine training requirements for Cyberspace/Information Technology Workforce line officers to ensure that they have the education and competencies needed to support the Department of the Navy's mission, goals, and dynamic workforce structure changes. Also, ensure that Cyberspace/Information Technology Workforce line officers can provide proper oversight over the enlisted Cyberspace/Information Technology Workforce.	O	Deputy Chief of Naval Operations (Information Dominance) (OPNAV N2/N6)	5/31/2015	

Recommendations							
Finding[27]	Rec. No.	Page No.	Subject	Status[28]	Action Command	Target or Actual Completion Date	Interim Target Completion Date[29]
2	6	33	Ensure Information Systems Technician/Information Systems Technician (Subsurface) Cyberspace/Information Technology Workforce enlisted personnel have pipeline training and career development reflecting current set of competencies and skills needed to perform Cyberspace/Information Technology Workforce work roles.	O	Deputy Chief of Naval Operations (Information Dominance) (OPNAV N2/N6)	5/31/2015	
2	7	35	Establish a centralized system to track and maintain a complete training history for Cyberspace/Information Technology Workforce personnel. This system should ensure that all source data systems which maintain electronic training and certification records are readily identifiable, and that training and certification records are maintained in cases for which records are not recorded on other systems.	O	Deputy Chief of Naval Operations (Information Dominance) (OPNAV N2/N6)	5/31/2015	
2	8	36	Establish procedures and related internal controls requiring that electronic or hard copy training records and certifications be retained for all Cyberspace/Information Technology Workforce active duty military members as required by SECNAV Manual M-5210.1, “Department of the Navy Records Management Program, Records Management Manual.”	O	Deputy Chief of Naval Operations (Information Dominance) (OPNAV N2/N6)	5/31/2015	
2	9	37	Until the centralized system is established as recommended in Recommendation 7, establish procedures and related internal controls requiring that all Cyberspace/Information Technology Workforce training records and certifications be recorded/entered into the Fleet Training Management and Planning System or Total Workforce Management System as required.	O	Deputy Chief of Naval Operations (Information Dominance) (OPNAV N2/N6)	5/31/2015	

Recommendations							
Finding[27]	Rec. No.	Page No.	Subject	Status[28]	Action Command	Target or Actual Completion Date	Interim Target Completion Date[29]
3	10	43	Require that all Navy commands with Cyberspace/Information Technology Work Force personnel include the Cyberspace/Information Technology Work Force in their assessable units for the Managers' Internal Control Programs and perform and document internal control evaluations for these assessable units using existing sources or separate evaluations, as required.	O	Department of the Navy Chief Information Officer	9/30/2014	
3	11	44	Ensure that management at all afloat activities are aware of their responsibilities for establishing, evaluating, and improving internal controls for the Cyberspace/Information Technology Workforce under the Managers' Internal Control Program.	O	Department of the Navy Chief Information Officer	9/30/2014	

Exhibit A:

Pertinent Guidance

Cyberspace Workforce

Secretary of the Navy (SECNAV) Instruction 3052.2, "Cyberspace Policy and Administration within DON," dated 6 March 2009, establishes policies and responsibilities for the administration of the Cyberspace/Information Technology Workforce (CS/ITWF) within the Department of the Navy (DON). It states that cyberspace capabilities are critical to achieving DON objectives in every war fighting domain and enterprise business model. Cyberspace operations will require intensive training and education for the total DON Cyberspace Workforce. The DON workforce will be a single integrated resource that is carefully managed with a dedicated focus on continued training and education to meet emerging technical developments. It also states the workforce will be employed to provide the highest level of cyberspace capabilities to meet Naval and joint objectives. The instruction notes that the DON Chief Information Officer (DON CIO) shall develop required Cyberspace Workforce policy and guidance. It also notes that DON CIO shall invest resources to recruit, train, retain, and equip personnel for cyberspace missions. Furthermore, the instruction states that with the Department of Defense (DoD) Chief Information Officer and Assistant Secretary of the Navy (Manpower and Reserve Affairs), DON CIO will track and measure the effectiveness of DON cyberspace manpower, personnel, training, and education programs.

SECNAV Instruction 1543.2, "Cyberspace/Information Technology Workforce Continuous Learning," dated 30 November 2012, states that its purpose is to establish policy and procedures for DON's CS/ITWF professional development through a Continuous Learning Program. This program is structured to support the continuing professional development of CS/ITWF personnel throughout their careers. The program will include education, training, certification, and other activities that support the sustainment and continued improvement of the capabilities of DON's CS/ITWF. The overarching goals of the program are to improve cyberspace operations and cyberspace mission effectiveness, and increase readiness across the cyberspace domain.

All civilian and military CS/ITWF personnel will participate in the Continuous Learning Program commensurate with their occupation, rank/grade, and position. The instruction specifically states that:

- DON CIO will identify measures for the evaluation of CS/ITWF continuous learning; and
- The Chief of Naval Operations shall:

- Develop and implement the CS/ITWF Continuous Learning Program within the Navy;
- Identify the CS/ITWF positions and personnel that are required to participate in the CS/ITWF Continuous Learning Program (which is all CS/ITWF personnel per this instruction); and
- Evaluate Continuous Learning Program effectiveness and compliance through assessments and formal inspector general inspections.

The instruction defines the CS/ITWF as military and Government civilians who plan, budget, manipulate, control, and archive information throughout its life cycle; develop, acquire, implement, evaluate, maintain, and retire information, information systems, and IT; develop the necessary policies and procedures; and apply measures that protect and defend information and information systems.

Cybersecurity Workforce

DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," dated 23 April 2007, establishes policy and assigns responsibilities for DoD information assurance (IA) training, certification, and workforce management. This guidance requires the heads of DoD components to "establish, resource, and implement IA training and certification programs for all DoD Component personnel in accordance with this policy and references. These programs shall train, educate, certify, and professionalize personnel commensurate with their responsibilities to develop, use, operate, administer, maintain, defend, and retire DoD Information Systems."

DoD Directive 8570.01-M, "Information Assurance Workforce Improvement Program," dated 24 January 2012, implements DoD Directive 8570.1 and provides guidance for the identification and categorization of positions and certification of personnel conducting IA functions within the DoD workforce supporting the DoD Global Information Grid per DoD Instruction 8500.2 (Reference (b)). The DoD IA workforce includes, but is not limited to, all individuals performing any of the IA functions described in this manual. Additional chapters focusing on personnel performing specialized IA functions, including certification and accreditation and vulnerability assessment, will be published as changes to this manual.

SECNAV Instruction 5239.2, "Department of the Navy Cybersecurity/Information Assurance Workforce Management, Oversight, and Compliance," dated 17 June 2010, states its purpose it to provide policy and assign responsibilities for the administration of the DON Cybersecurity/Information Assurance Workforce Management Oversight and Compliance Program.

SECNAV Instruction M-5239.2, "DON Information Assurance Workforce (IAWF) Management Manual," dated 29 May 2009, provides a high level policy for IAWF management, describes DON IAWF management plans, establishes DON IAWF oversight and management reporting requirements to support implementation, and establishes IA awareness requirements for information system users.

DON CIO Memo, "Guidance for Cybersecurity Workforce Operating System/Computing Environment Certification Compliance Process," dated 8 February 2012, provides updated guidance for DON IAWF commercial operating system/computing environment certification requirements.

Training/Manpower

Chief of Naval Operations (OPNAV) Instruction 3120.32D, "Standard Organization and Regulations Manual (SORM)," dated 16 July 2012, states that its purpose is to reissue regulations and guidance governing the conduct of all members of the U.S. Navy. The regulations and guidance are for the internal operation of DON only and create no right or benefit, substantive or procedural, enforceable at law against the United States, DoD, or DON.

OPNAV Instruction 3500.34F, "Personnel Qualification Standards (PQS) Program," dated 13 June 2005, issues policy, procedures, and responsibilities for the PQS program. The PQS program ensures personnel demonstrate required competencies prior to performing specific duties. PQS delineates the minimum knowledge and skill sets an individual must demonstrate before standing watches or performing other specific duties necessary for the safe, secure, and proper operation of a ship, aircraft, or support system. This instruction is intended for use by commanding officers and officers in charge for implementing and managing a PQS qualification program.

OPNAV Instruction 1500.74A, "Utilization of Enlisted Occupational Standards for Training and Career Development," dated 26 January 2007, establishes guidelines for utilization of enlisted occupational standards (OCCSTDS) as a basis for training and career development. OCCSTDS provide the most logical standards for training objectives by providing a snapshot of performance tasks required of Navy enlisted personnel. OCCSTDS are based on data collected from a variety of sources (Fleet units, warfare requirements, rating advisors, enlisted community managers, warfare sponsors, etc.) through the Navy Skills Management System (SMS) process, and are approved by the resource sponsor/warfare sponsor prior to publication. Although several curriculum development methods/approaches (such as task analysis and Personnel Performance Profiles) may be used to develop training curriculum, OCCSTDS will be used as the primary basis for: (1) preparation of formal school curricula (except for certain NEC-producing or sponsor-stated requirements) and onboard training, including formal onboard training packages and on-the-job training, (2) development of Personnel

Advancement Requirements, (3) development of Navy-wide advancement examinations, and (4) development of nonresident training packages (e.g., rate training manuals).

OPNAV Instruction 1500.77, "Learning and Development Roadmap for Enlisted Sailors," dated 14 December 2009, **dated 14 December 2009,** establishes policy for the development, utilization, and maintenance of the Learning and Development Roadmaps for enlisted Sailors. Learning and Development Roadmaps support all active and reserve component military members and are a valuable tool for recruiting, advancement, and retention. Learning and Development Roadmaps provide enlisted personnel with a comprehensive career guide, listing learning and development objectives, as well as milestones for the completion of these objectives by pay grade and rating.

Navy Enlisted Manpower and Personnel Classifications and Occupational Standards (NEOCS) Manuals I and II, Navy Personnel Command (NAVPERS) 18068F, **dated April 2013 and January 2013**, states that the Navy Enlisted Occupational Classification System (NEOCS) provides the means by which all Navy enlisted personnel are classified. To support enlisted personnel planning, procurement, training, promotion, distribution, assignment, and mobilization within that classification system, the Navy has established specific standards. These standards define minimum skill and knowledge requirements for enlisted personnel at each pay grade and within each career field. Volume I of this manual contains an introductory overview of NEOCS, an explanation of Naval Standards and Occupational Standards, and pertinent appendixes. It also contains individual chapters with the Occupational Standards for each rating. Volume II of this manual includes an explanation of the Navy Enlisted Classification structure, a listing of those classifications, and related appendixes.

NAVPERS 15839I, Volume 1, "Manual of Navy Officer Manpower and Personnel Classifications," dated January 2013, states its purpose is to explain the Navy Officer Occupational Classification System codes and other code structures and established abbreviations used to identify the qualitative needs for officer manpower and for reporting and recording officer qualifications and other personnel data.

Records Management

SECNAV Instruction 5210.8D, "Department of the Navy Records Management Program," dated 31 December 2005, provides policy and assigns responsibilities for the life-cycle management (creation, maintenance, use, and disposition) of information as records in all media, including electronic. It also establishes responsibility for the DON Records Management Program. It states that it is DON policy to:

a. "Create, maintain, and preserve information as records, in any media, that document the transaction of business and mission to provide evidence of DON organization, functions, policies, procedures, decisions, and operational, logistical, and support transactions and other activities."

b. "Manage records effectively and efficiently. Economical, efficient, and reliable means shall be used for creation, retrieval, maintenance, preservation, and disposition of records in any media."

It further states that the Chief of Naval Operations is required to implement the DON Records Management Program within the Navy.

SECNAV Manual M-5210.1, "Department of the Navy Records Management Program, Records Management Manual," dated May 2012, provides guidelines and procedures for the proper administration of a records management program.

Part I, "Authority and Procedures for Records Disposition Program," Paragraph 17, "Electronic Records," states, "Any information created, received, transmitted, maintained, or managed as an organization record that can be read by using a computer or any other electronic device, that satisfies the definition of a Federal record, shall be considered an electronic record." It further states, "Before a document is created on an electronic records system that will maintain the official file copy, each document must be identified sufficiently to enable authorized personnel to retrieve, protect, and dispose of it."

Part III, Chapter 1, "Military Personnel Records" states that "the records described in this chapter pertain to the supervision and administration of military personnel and military personnel affairs." This includes training of personnel. It further states, "Retention periods prescribed in this chapter are applicable to military personnel records of Navy and Marine Corps activities and offices throughout the DON." Part III, Chapter 1, SSIC 1500, "Training and Education Records," shows different retention requirements for various types of enlisted personnel and officer records showing completion of training.

Exhibit B:

Scope and Methodology

We conducted an audit of the Cyberspace/Information Technology skills sets for active duty military personnel at selected commands from 11 December 2012 to 1 April 2014 (please see Exhibit C for a list of activities visited and/or contacted). We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our evaluation of whether the Department of the Navy (DON) had established key procedures and internal controls to clearly delineate the Cyberspace/Information Technology Workforce (CS/ITWF) as required by Secretary of the Navy guidance covered procedures and internal controls during the audit period of 11 December 2012 to 1 April 2014 (Finding 1). Our evaluation of whether CS/ITWF personnel were technically proficient in their current IT-related functions was based on related training/certifications they had received as of the time of our site visits for the 15 audited activities. These site visits occurred at different times (Finding 2). We evaluated whether the 15 audited activities' Managers' Internal Control Programs (MICPs) covered CS/ITWF in their assessable units for FY 2013 (Finding 3).

We evaluated internal controls and reviewed compliance with established laws and regulations. Our detailed evaluation of internal controls, and laws and regulations is shown in Findings 1-3. Overall, we determined whether DON had established key procedures and internal controls to clearly delineate the CS/ITWF as required by Secretary of the Navy guidance. Specifically, we determined whether DON: (1) uniformly defined the Navy's total CS/ITWF and identified which officer and enlisted personnel occupations comprised the CS/ITWF; (2) ensured that the CS/ITWF definition was communicated to all levels within the Navy; and (3) established an accurate, comprehensive database of all CS/ITWF military personnel (Finding 1). We interviewed activity personnel and reviewed relevant documentation to determine whether internal controls over the management of Cyberspace/IT skill sets were sufficient to ensure Navy Cyberspace/IT active duty personnel were technically proficient in their current IT-related functions in accordance with regulations (Finding 2). We determined whether the CS/ITWF was included as an assessable unit in MICPs in accordance with relevant MICP regulations (Finding 3).

We reviewed Fiscal Year (FY) 2009-2011 cyber-related audit reports published by the Government Accountability Office, Department of Defense (DoD) Inspector General, and Naval Audit Service. We did not find any reports on which to follow up.

The following shows our detailed scope and methodology by finding, and our results concerning data reliability.

CS/ITWF Definition and Personnel Database (Finding 1)

To determine relevant criteria defining the total CS/ITWF and identify what military occupations comprise this workforce, we: searched the DON Chief Information Officer (DON CIO) Web site; reviewed FY 2009-2011 cyber-related audit reports published by the Government Accountability Office, DoD Inspector General, and Naval Audit Service; reviewed DON CIO PowerPoint slides presented at the DON CIO 2012 IT East Coast Conference held 15 May – 17 May 2012 at Virginia Beach, VA; and reviewed the Navy Credentialing Opportunities Online (Navy COOL) Web site.[30] We also interviewed personnel from: DON CIO; Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) Zero-Based Review Task Force; the Navy Cyber Forces Command; and the Naval Computer and Telecommunications Area Master Station Atlantic.

To determine whether a comprehensive database of on-hand Navy CS/ITWF personnel was available, we interviewed personnel from: DON CIO; OPNAV N2/N6; the Bureau of Naval Personnel; and the Navy Manpower Analysis Center, Naval Personnel Command.

Training of Navy CS/ITWF Personnel (Finding 2)

***Training and Certification Guidance*.** To identify relevant cyberspace operations training and certification guidance, we reviewed:

- The DON CIO and Navy Personnel Command Web sites;
- Cyberspace-related audit reports published 2009 through 2011 by the Government Accountability Office, Department of Defense Inspector General, and Naval Audit Service;

[30] Navy COOL is a Web site, designed for Navy service members, that defines civilian credentials that best map to Navy ratings, jobs, designators, and collateral duties/assignments. It outlines the path, work, training, and experience required to achieve them. It defines comprehensive information on occupational credentials — including certifications, licenses, apprenticeships, and growth opportunities — correlating with every Navy rating, job, designator, and collateral duty/out of rate assignment.

- Several DoD and DON workforce related criteria[31]; and
- PowerPoint presentations from the DON CIO 2012 IT East Coast Conference.

We also interviewed personnel from the office of the DON CIO and from the Navy Cyber Forces Command.

Universe. The Office of Chief of Naval Operations' (OPNAV's) Zero-Based Review Task Force provided us a baseline Total Force Manpower Management System (TFMMS) database[32] of the Navy's authorized billets, dated 18 October 2012. The universe contained 32,938 validated (verified by the Task Force based on database review by Navy commands) cyber, non-cyber, funded, non-funded, civilian, contractor, active duty, and Navy Reserve TFMMS Fiscal Year (FY) 2013 billets for 32 Budget Submitting Offices (BSOs). Our review of the OPNAV N2/N6 Zero-Based Review Task Force database (in conjunction with discussions with DON CIO, Zero-Based Review Task Force, and Navy Cyber Forces Command management personnel) showed that the validated Zero-Based Review database was the most comprehensive record available to identify the total CS/ITWF. However, it only showed authorized billets, not on-hand personnel.

Because of the database's wide array of billets, we solicited feedback from DON CIO and Naval Computer and Telecommunications Area Master Station Atlantic[33] personnel to reduce our scope. Based on their feedback that we should first address Fleet military personnel, we determined that focusing on the Navy's active duty military personnel at selected commands would yield the best results. To identify the active CS/ITWF billets, we filtered the baseline database to remove all non-cyber and non-funded billets for FY 2013. This resulted in identifying 27,405 CS/ITWF billets. Of the 27,405 CS/ITWF billets: 15,897 (58 percent) represented the total active duty military CS/ITWF billets discussed below; 178 (1 percent) represented reserve military billets; 10,968 (40 percent) were civilian billets; and 362 (1 percent) were contractor billets.

TFMMS maintains billet data, not on-hand personnel information. Therefore, we filtered the baseline database to identify the BSOs and activities assigned the most active duty CS/ITWF billets. This was accomplished by first filtering the data to remove all non-cyber, non-funded, civilian, and contractor billets. This identified 16,075 military

[31] These criteria include: OPNAV Instruction 1500.74A, "Utilization of Enlisted Occupational Standards for Training and Career Development," dated 26 January 2007; OPNAV Instruction 1500.77, "Learning and Development Roadmap for Enlisted Sailors," dated 14 December 2009; SECNAV Instruction 3052.2, "Cyberspace Policy and Administration within the DON," dated 6 March 2009; SECNAV Instruction 5239.2, "DON Cybersecurity/Information Assurance Workforce Management, Oversight, and Compliance," dated 17 June 2010; SECNAV Manual 5239.2, "DON Information Assurance Workforce Management Manual," dated 29 May 2009; DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," dated 23 April 2007; DoD Directive 8570.01-M, "Information Assurance Workforce Improvement Plan," dated 24 January 2012; SECNAV Instruction 1543.2, "Cyberspace/IT Workforce Continuous Learning," dated 30 November 2012.

[32] Maintained by the Bureau of Naval Personnel.

[33] First activity we audited.

CS/ITWF billets. We then removed the 178 Navy Reserve cyber billets under the Commander, Navy Reserve Force Command (BSO 72), from the identified military CS/ITWF billets, to ensure only active duty CS/ITWF billets were represented. Of the remaining 15,897 active duty CS/ITWF billets, 14,567 (92 percent) represented active duty enlisted billets and 1,330 (8 percent) represented active duty officer billets. The 15,897 active duty CS/ITWF billets were then sorted by Major Claimant to identify the BSOs and activities with the largest amount of active duty CS/ITWF billets. Of the 32 total BSOs, we identified U.S. Fleet Forces Command, U.S. Pacific Fleet, Naval Education and Training Command, and Naval Special Warfare Command as the BSOs with the largest number of active duty CS/ITWF billets. These four commands accounted for 13,598 (85.5 percent) of the 15,897 active duty billets; the 13,598 billets were dispersed amongst 923 activities.

Table 6. BSOs with Largest Amount of Active Duty CS/ITWF Billets

Major Claimant	BSO	Activities	Active Duty Billets	% of Active Duty Population
U.S. Fleet Forces Command	60	452	8,152	51.3
U.S. Pacific Fleet	70	349	3,225	20.3
Naval Education and Training Command	76	46	1,357	8.5
Naval Special Warfare Command	88	76	864	5.4
Total		**923**	**13,598**	**85.5**

Sampling Methodology. To determine the most appropriate sampling methodology, we consulted the Naval Audit Service statistician. The statistician determined that statistical sampling of afloat and shore activities would be too large and inflexible to satisfy our audit objective. As a result, he recommended we use a judgmental sampling approach throughout the audit.

Site Sample Selection. Initially, we intended to judgmentally select activities from each of the four cited BSOs with the largest number of active duty CS/ITWF billets to conduct site visits. However, limited travel funds caused by the sequestration necessitated that we localize our approach. This reduction in scope again prompted us to solicit recommendations from DON CIO regarding the types of activities to include in our audit scope. In an effort to obtain the best coverage of active duty CS/ITWF personnel and address DON CIO's recommendations, we decided to modify the scope to only include local activities[34] under U.S. Fleet Forces Command (BSO 60) and Space and Naval Warfare Systems Command (BSO 39). U.S. Fleet Forces Command remained in our scope because it was the BSO with the largest number of active duty CS/ITWF billets. This was because of the proximity of its ship, submarine, and shore activities, as well as

[34] Norfolk, VA; Virginia Beach, VA; and Newport News, VA.

the fact that it contained the types of activities recommended for review by DON CIO. These activities included large, medium, and small afloat vessels, as well as Operational and Type Commands. The Space and Naval Warfare Systems Command (195 active duty CS/ITWF billets) was added as a DON CIO priority due to the command's role in Information Dominance and its local activities. Both BSOs accounted for a total of 8,347 (53 percent) of the 15,897 active duty CS/ITWF billets.

A total of 15 ashore and afloat activities were judgmentally selected for U.S. Fleet Forces Command and Space and Naval Warfare Systems Command. Local ashore activities with the largest amount of active duty CS/ITWF billets were judgmentally selected from the validated TFMMS database. Afloat activities were selected from lists provided by Commander, Naval Air Forces Atlantic; Commander, Naval Surface Forces Atlantic; and Commander, Submarine Force Atlantic. These commands provided the availability of all local surface and submarine vessels that would be in-port during the period of our site visits, 1 March 2013 to 31 May 2013. For U.S. Fleet Forces Command, we selected Naval Computer and Telecommunications Area Master Station Atlantic, Norfolk, VA, because it contained the largest amount of active duty CS/ITWF billets in the local area. We then selected Naval Cyber Defense Operations Command, Virginia Beach, VA, as a medium-range ashore activity and Navy Cyber Forces Command, Virginia Beach, VA, as a low-range ashore activity.[35] Two aircraft carriers, two destroyers, four submarines, one frigate, and one cruiser were also selected as medium- and low-range afloat activities.

For the Space and Naval Warfare Systems Command, we selected two ashore activities: Space and Naval Warfare Systems Command Space Center Tidewater, VA, and Space and Naval Warfare Systems Command Space Field Activity, Chantilly, VA. These two activities had the highest number of active duty CS/ITWF billets, and the Tidewater activity was local. Because of their size, they were categorized as low-range activities.

Overall, we selected 5 ashore activities which comprised 784 (5 percent) of the total 15,897 active duty billets, and 10 afloat activities which comprised 243 (2 percent) of the total 15,897 active duty billets. The 15 activities together included a total of 1,027 (7 percent) of the 15,897 active duty billets. Of these, 911 were enlisted active duty billets, and 116 were officer active duty billets. Overall, as noted, the 15 activities were judgmentally selected based on: the number of active duty billets, the location of activities, our agency statistician's recommended sampling approach, and DON CIO recommendations. These 15 judgmentally selected ashore and afloat activities are in Table 7.

[35] As shown in Findings 2 and 3, Naval Computer and Telecommunications Area Master Station Atlantic, Norfolk, VA and Naval Cyber Defense Operations Command, Virginia Beach, VA are actually under the operational control of U.S. Fleet Cyber Command. Navy Cyber Forces Command, Virginia Beach, VA is under the operational command of the U.S. Fleet Forces Command.

Table 7. Selected Ashore and Afloat Activities from BSOs 60 and 39					
Selected Activities	**Range**	**Enlisted**	**Officer**	**Total Billets**	**Percentage of Active Duty Billets**
BSO 60 – U.S. Fleet Forces Command		7,524	628	8,152	51%
Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT)	High	375	29	404	
Navy Cyber Defense Operations Command (NCDOC)	Medium	198	13	211	
Navy Cyber Forces Command	Low	44	43	87	
Ashore Activity Totals		**617**	**85**	**702**	4%
USS George H.W. Bush (CVN77)	Medium	95	6	101	
USS Theodore Roosevelt (CVN 71)	Medium	84	6	90	
USS Cole (DDG 67)	Low	12	0	12	
USS Boise (SSN 764)	Low	0	0	0	
USS Montpelier (SSN 765)	Low	0	0	0	
USS Newport News (SSN 750)	Low	1	0	1	
USS Scranton (SSN 756)	Low	0	0	0	
USS Vella Gulf (CG 72)	Low	14	0	14	
USS Elrod (FFG 55)	Low	10	0	10	
USS Bulkeley (DDG 84)	Low	15	0	15	
Afloat Activity Totals		**231**	**12**	**243**	2%
BSO 39 – Space and Naval Warfare Command (SPAWAR)					
SPAWAR Systems Center Atlantic	Low	33	16	49	
SPAWAR Space Field Activity Chantilly	Low	30	3	33	
SPAWAR (All Ashore) Activity Total		**63**	**19**	**82**	1%
Total Ashore Active Duty Billets		**680**	**104**	**784**	5%
Total Afloat Active Duty Billets		**231**	**12**	**243**	2%
Total Activities	**15**	**911**	**116**	**1,027**	**7%**

Personnel Sample Selection and Review. Prior to our site visit, we required that each command provide a personnel roster of their entire CS/ITWF[36] to include name, rate, rank, whether or not personnel were part of the Information Assurance Workforce (IAWF), time on-board, job title, and primary and subsequent Navy Enlisted Classifications (NECs) or Navy Officer Billet Codes (NOBCs). This information was then used to judgmentally select personnel to be interviewed while we were on-site. To effectively communicate who should be included on the roster, we sent each activity correspondence containing the Zero-Based Review CS/ITWF definition,[37] as well as a listing of the NECs, NOBCs, and ratings considered to be part of the CS/ITWF on the

[36] Finding 1 shows there was no database of on-hand CS/ITWF personnel at activities.

[37] Navy Cyber Workforce Zero-Based Review CS/ITWF definition approved by the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6), dated April 2012, states, "The Navy-wide Cyber workforce is comprised of the Navy's Total Force (military [AC, RC], civilian and contractor personnel) who conduct operations in cyberspace as a part of their job responsibilities. Each member of the workforce will support one or more cyber functions and be classified by their requirement for mission success. Many Navy personnel use cyberspace in the execution of their duties, but are not conduction cyber operations. Therefore, they are not part of the cyber workforce (e.g., SIGINT [signals intelligence] collections, SIGINT/ISR [intelligence, surveillance, and reconnaissance] administration, ISR connectivity, etc…)."

Navy Credentials Opportunities On-Line (COOL)[38] Web site.[39] We also explained to activity personnel that individuals with NECs 2790 (Information Systems Technician (IAT I)) and/or 2791 (Information Systems Administrator (IAT II)) must be included on the roster. These two NECs were not yet added to Navy COOL's Web site at the time of our site visits.

At each activity, we evaluated the skill sets of no more than 10 enlisted and officer active duty personnel (if fewer than 10 CS/ITWF active duty personnel were at an activity, we evaluated all of those personnel). We judgmentally selected the interviewees to get a cross section of ratings, time at command, ranks, members that were and were not part of the Cybersecurity Workforce portion of the CS/ITWF, and work roles. This was accomplished by interviews, work role templates, and training documentation. Work role templates were created by us for all selected personnel based on their NEC/NOBC and job title provided on the roster. Different types of templates were created to interview the various types of ratings, rankings, NECs/NOBCs, and current work roles.

The templates were used during each interview. We asked questions pertaining to each individual's current work role and training to determine if they had the necessary skill sets to perform in their current IT-related capacity. Templates were created by pulling questions from the NEC/NOBC and/or work roles' occupational definitions found in the Naval Personnel Instruction 18068F, "Manual of Navy Enlisted Manpower and Personnel Classifications and Occupational Standards Volumes I and II," dated January 2013. When occupational definitions were not found in the manuals, we either searched the Internet for descriptions or asked the activity points of contact whether they maintained work role descriptions for their particular activity. If the activities did not maintain descriptions, we gained an understanding of selected personnel's work role on-site and asked our standard questions in reference to their current role. In addition to the questions pulled directly from each person's NEC, NOBC, and/or current work role descriptions, all templates contained the following standard questions:

1. Have you received training to help you be proficient in performing your current role?
2. Are there any parts of your job you feel you need additional training or skills to accomplish your roles and responsibilities?

[38] Navy COOL is a Web site, designated for Navy service members, that defines civilian credentials that best map to Navy ratings, jobs, designators, and collateral duties/assignments. It outlines the path, work, training and experience required to achieve them. It defines comprehensive information on occupational credentials — including certifications, licenses, apprenticeships, and growth opportunities — correlating with every Navy rating, job, designator, and collateral duty/out-of-rate assignment.

[39] Navy Officer: 1820 - Information Professional, 1840 – Cyber Warfare Engineers, 6420 - Limited Duty Officer Information Systems, 7421 - Warrant Officer Information Systems Technician. Navy Enlisted: All enlisted Navy with following Navy Enlisted Classification Codes (NECs) (most should be IT and ITS Ratings, some ET, FT, FC, CTM, CTN): IT - Information Systems Technician, ITS - Information Systems Technician (Subsurface), ET - Electronics Technicians, FT - Fire Control Technicians, FC - Fire Controlman, CTM - Cryptologic Technician Maintenance, and CTN - Cryptologic Technician Networks. The list of NECs/NOBCs is in Finding 1.

3. Do you work on new or legacy systems/programs?
4. Are you required to have any certifications in your current work role? Have you had any required certifications expire?
5. What type of training have you received while at the Command in your current Cyberspace/IT-related position?
6. Do you believe the training you received was helpful for performing your current duties? If not, what type of training is needed to better prepare you to perform your duties in your current position?

We also requested each activity and/or interviewee provide us documentation showing training received by each interviewee to determine whether the selected personnel were provided with and successfully completed the training necessary to perform their current IT-related functions. Some examples of training documentation include commercial vendor certificates, Personnel Qualification Standards, and NEC graduation certificates.

A total of 116 personnel were interviewed across the 15 activities. Of these 116, 20 were officers, and 96 were enlisted personnel. We judgmentally selected the interviewees to get a cross section of ratings, time at command, ranks, members that were and were not part of the Cybersecurity Workforce portion of the CS/ITWF, and work roles. Of the 96 enlisted personnel, we interviewed 74 individuals with the Information System Technicians (ITs) or Information Systems Technician (Subsurface) (ITS) ratings, 7 Cryptologic Technician Networks (CTNs), 2 Cryptologic Technician Collections (CTRs), 1 Information Specialist (IS), 8 Electronics Technicians (ETs), 3 Fire Controlmen (FC), and 1 Sonar Technician Surface (STG). Table 8 shows a breakdown of the types of individuals interviewed at each activity.

Table 8. Interviewed Personnel at Selected Ashore and Afloat Activities from BSOs 60 and 39

Selected Activities	Personnel Interviewed	Enlisted	Officer	IT/ITS	CTN	CTR	IS	ET	FC	STG
BSO 60 – U.S. Fleet Forces Command										
Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT)	10	7	3	7	0	0	0	0	0	0
Navy Cyber Defense Operations Command (NCDOC)	10	8	2	4	3	1	0	0	0	0
Navy Cyber Forces Command	10	8	2	7	0	0	1	0	0	0
Ashore Activity Totals	**30**	**23**	**7**	**18**	**3**	**1**	**1**	**0**	**0**	**0**
USS GEORGE H.W. BUSH (CVN 77)	10	8	2	8	0	0	0	0	0	0
USS THEODORE ROOSEVELT (CVN 71)	10	7	3	5	0	0	0	2	0	0
USS COLE (DDG 67)	10	8	2	5	0	0	0	2	1	0
USS BOISE (SSN 764)	1	1	0	1	0	0	0	0	0	0
USS MONTPELIER (SSN 765)	3	3	0	2	0	0	0	1	0	0
USS NEWPORT NEWS (SSN 750)	2	2	0	1	0	0	0	1	0	0
USS SCRANTON (SSN 756)	4	4	0	4	0	0	0	0	0	0
USS VELLA GULF (CG 72)	10	6	4	6	0	0	0	0	0	0
USS ELROD (FFG 55)	7	7	0	6	0	0	0	1	0	0
USS BULKELEY (DDG 84)	10	10	0	5	0	1	0	1	2	1
Afloat Activity Totals	**67**	**56**	**11**	**43**	**0**	**1**	**0**	**8**	**3**	**1**
BSO 39 – SPAWAR										
SPAWAR Space Center Tidewater	10	9	1	9	0	0	0	0	0	0
SPAWAR Space Field Activity Chantilly	9	8	1	4	4	0	0	0	0	0
SPAWAR (All Ashore) Activity Total	**19**	**17**	**2**	**13**	**4**	**0**	**0**	**0**	**0**	**0**
TOTAL	**116**	**96**	**20**	**74**	**7**	**2**	**1**	**8**	**3**	**1**

Department of the Navy Managers' Internal Control Program (MICP) (Finding 3)

To evaluate whether the CS/ITWF was included as an FY 2013 assessable unit in Managers' Internal Control Programs, we interviewed management personnel for each of the ships and submarines we visited, as well as at Echelon III command level Immediate Superior in Commands (ISICs) for ships and submarines reviewed.[40] We also interviewed MICP coordinators at each of the shore activities visited. Additionally, we obtained supporting assessable unit listings. We did this to determine whether:

- Ship managers were aware of the MICP;
- Assessable units at some level included CS/ITWF;

[40] We found that the three Echelon II commands we reviewed, U.S. Fleet Forces Command, U.S. Fleet Cyber Command, and SPAWAR, submit MIC certification statements to the office of the Chief of Naval Operations, and in turn require subordinate activities to submit MIC certification statements to them. The overall MIC certification statement is primarily developed from the individual submissions from the Type Commanders (TYCOMs)/Immediate Superior in Commands (ISIC) who gather documentation from their subordinate commands. The ISICs submit required documentation to the Echelon II Command MICP coordinator.

- The management control plan included only the cybersecurity/information assurance portion of CS/ITWF;
- The management control plan did not include CS/ITWF; and
- If CS/ITWF was in fact included as in assessable unit, was any form of management control evaluations performed for the assessable unit?

Data Reliability.

Data reliability was not an objective of the audit. We obtained Total Force Manpower Management System data from the Zero-Based Review Task Force. However, we did not test the data because doing so was beyond the scope of this audit.

Exhibit C:

Activities Visited and/or Contacted

ACTIVITY	LOCATION
Department of the Navy Chief Information Officer (DON CIO)	Washington, DC
Chief of Naval Operations for Information Dominance (OPNAV N2/N6)	Washington, DC
U.S. Fleet Forces Command	Norfolk, VA
U.S. Fleet Cyber Command/US 10th Fleet	Fort Meade, MD
Space and Naval Warfare Command (SPAWAR)	San Diego, CA
Naval Education Training Command (NETC)	Pensacola, FL
Center for Information Dominance	Pensacola, FL
Naval Education Training Professional Development Technology Center (NETPDTC)	Pensacola, FL
Bureau of Naval Personnel	Millington, TN
Commander, Naval Air Forces Atlantic	Norfolk, VA
Commander, Naval Surface Force, U.S. Atlantic Fleet	Norfolk, VA
Commander, Submarine Force Atlantic Fleet	Norfolk, VA
Navy Cyber Forces Command*	Virginia Beach, VA
Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT)*	Norfolk, VA

Navy Cyber Defense Operations Command*	Virginia Beach, VA
SPAWAR Space Field Activity*	Chantilly, VA
SPAWAR Systems Center (SPAWARSYSCEN) Atlantic*	Norfolk, VA
USS GEORGE H. W. BUSH (CVN 77)*	Norfolk, VA
USS THEODORE ROOSEVELT (CVN 71)*	Newport News, VA
USS BULKELEY (DDG 84)*	Norfolk, VA
USS COLE (DDG 67)*	Norfolk, VA
USS ELROD (FFG 55)*	Norfolk, VA
USS VELLA GULF (CG 72)*	Portsmouth, VA
USS BOISE (SSN 764)*	Norfolk, VA
USS MONTPELIER (SSN 765)*	Norfolk, VA
USS NEWPORT NEWS (SSN 750)*	Norfolk, VA
USS SCRANTON (SSN 756)*	Norfolk, VA

*Activities Visited

Exhibit D:

Sources Showing Who Makes Up the Cyberspace/Information Technology Workforce

We found five sources that communicated to Navy personnel who make up the Cyberspace/Information Technology Workforce (CS/ITWF) for Navy personnel. Secretary of the Navy Instruction 1543.2, "Cyberspace/Information Technology Workforce Continuous Learning," dated 30 November 2012, provides the only official Navy definition of who makes up the overall CS/ITWF. Details from the five sources are provided in the table below:

Sources Showing Who Makes Up the CS/ITWF	
Source	**Excerpts from Source**
Department of the Navy Chief Information Officer (DONCIO) Web site article, dated 27 March 2008	"The CS/ITWF includes military and government civilians who plan, budget, manipulate, control and archive information throughout its life cycle; develop, acquire, implement, evaluate, maintain and retire information, information systems and IT; develop the necessary policies and procedures; and apply measures that protect and defend information and information systems."
"DON Cyber/IT Workforce Strategic Plan FY2010-2013," published July 2010	"Employees who carry out work on a daily basis that falls into one or more of the following areas: ▪▪ **Manage:** Functions that concern overseeing a program or other aspects of a cyber, security, or technical program at a high level and ensuring its currency with changing risk and threat. ▪▪ **Design:** Functions that concern scoping a Cyber/IT program or developing procedures and processes that guide work execution at the program and/or system level. ▪▪ **Implement:** Functions that concern putting Cyber/IT programs, processes, or policy into action within an organization, either at the program or system level. ▪▪ **Evaluate:** Functions that concern assessing the effectiveness of a cyber program, policy, or process in achieving its objectives. The workforce is further broken down into three categories depending on the amount of time spent carrying out information tasks. The three groupings are defined as: ▪▪ **Core Cyber/IT Professionals:** Those personnel who are responsible for providing cyber capabilities needed across the Department of the Navy (DON). They require specialized and concentrated competencies, reinforced with foundational and continual training and education. ▪▪ **Expert Users:** Those employed in jobs for which they require an increased knowledge of the cyberspace domain and cyber war fighting mission. Their required level of IT expertise is specifically associated with the jobs they need to accomplish. ▪▪ **Information System Users:** Those who require foundational IT skills, including the use of word processing, e-mail, online research tools, Web, and decision making aids. For these individuals — who include virtually every member of DON — IT is a tool required to execute their primary jobs. Note: this group is not part of the Cyber/IT Workforce."

Secretary of the Navy Instruction 1543.2, "Cyberspace/Information Technology Workforce Continuous Learning," dated 30 November 2012	Reiterates the CS/ITWF definition identified in the 27 March 2008 DON Chief Information Officer article. However, this definition more clearly defines the CS/ITWF by listing the rates, Naval Officer Billeting Codes (NOBCs), and Navy Enlisted Classifications (NECs) that qualify for professional development through a Continuous Learning Program. **Navy Officer (4 NOBCs)** 1820 - Information Professional 1840 – Cyber Warfare Engineers 6420 - Limited Duty Officer Information Systems 7421 - Warrant Officer Information Systems Technician **Navy Enlisted Ratings (2 ratings)** IT - Information Systems Technician ITS - Information Systems Technician (Subsurface)
Deputy Chief of Naval Operations For Information Dominance (OPNAV N2/N6) Zero Based Review Report, dated April 2012[41]	"The Navy-wide Cyber Workforce is comprised of the Navy's Total Force (military, civilian, and contractor personnel) who conducts operations in cyberspace as a part of their job responsibilities. Each member of the workforce will support one or more cyber functions and be classified by their requirement for mission success. Many personnel using cyberspace in the execution of their duties, but are not conducting cyber operations are not part of the cyber workforce." This report includes NOBCs, NECs and enlisted ratings shown in Secretary of the Navy Instruction 1543.2, as well as 20 additional NOBCs, 38 additional NECs,[42] and 22 additional enlisted ratings.
Navy Credentialing Opportunities Online (COOL) Web site[43]	"Personnel, whether performing Information Assurance/Computer Network Defense (IA/CND) duties in the Information Management/Information Technology (IM/IT), Command, Control, Computers and Communications (C4), acquisition, administration, aviation, combat systems, intelligence, logistics, medical, submarine, surface or any other functional commands, are required to hold the appropriate training targeted to the IT environment specified in the Department of Defense 8570.01-M. The CS/ITWF/Information Assurance Workforce (IAWF) includes any uniformed military, civilian, or contractor personnel who have privileged access or major CS/ITWF/IAWF management responsibilities. Note, not all personnel holding the below series are in the CS/ITWF/IAWF, but personnel holding these series have been identified as performing CWSF/IAWF functions. The following personnel are considered to be part of the CS/ITWF/IAWF." Active duty personnel considered to be part of the CS/ITWF/IAWF include: "All Navy Officers performing Cyberspace/Information Assurance duties. All Information Professional (IP) Officers to include Limited Duty Officer (LDO) and Warrant are Information Assurance Manager (IAM) Level 2 personnel and must be registered and certified as such (regardless of

[41] The report's purpose section states, "Given the critical importance of building and maintaining a proficient and resilient cyber workforce, the Navy-wide Cyber Zero-Based Review was initiated in September 2011 to establish a baseline of the Navy's current cyber workforce based on present requirements and inform the development of an executable Cyber Warfare Manpower Strategy."

[42] The Continuous Learning criteria did not list any NECs as being part of the CS/ITWF.

[43] Navy COOL is a Web site for Navy service members that defines civilian credentials which best map to Navy ratings, jobs, designators, and collateral duties/assignments. It outlines the path, work, training, and experience required to achieve them. It defines comprehensive information on occupational credentials — including certifications, licenses, apprenticeships, and growth opportunities — correlating with every Navy rating, job, designator, and collateral duty/out of rate assignment.

	size of network/facility being managed or operated). Specifically, Officers with: **Navy Officer** 1820 - Information Professional 1840 – Cyber Warfare Engineers 6420 - Limited Duty Officer Information Systems 7421 - Warrant Officer Information Systems Technician **Navy Enlisted** All Enlisted Navy with following Navy Enlisted Classification Codes (NECs) (most should be IT and ITS Ratings, some ET, FT, FC, CTM, CTN): **IT - Information Systems Technician** **ITS - Information Systems Technician (Subsurface)** **ET - Electronics Technicians** **FT - Fire Control Technicians** **FC - Fire Controlman** **CTM - Cryptologic Technician Maintenance** **CTN - Cryptologic Technician Networks** 0509 - AN/SQQ-89 (V) Adjunct Subsystem Level II Technician 0510 - AN/SQS-53D Sensor Subsystem Level II Technician/Operator 0522 - AN/SQQ-89(V) 15 Sonar System Level II Technician 0525 - AN/SQQ-89A (V)15 Surface Ship USW Combat Systems Maintenance Technician 1104 - AEGIS Combat System (BL4) Maintenance Supervisor 1136 – TTWCS Operation and Maintenance (O&M) Technician 1144 - AEGIS Combat System (BL 4) Computer System Maintenance Technician 1318 - AEGIS Computer Network Technician, Track II 1331 - AEGIS Weapons System Technician (TK IV) 1332 - Over the Horizon-Targeting (OTH-T) Supervisor 1335 - UYQ-70 Computer/Display LAN Technician 1336 - AEGIS Weapons Systems Technician TRACK 3 1493 - Tactical Support Communications (TSCOMM) Replacement Program Maintenance Technician 1654 - Intelligence Center Maintenance Technician 1678 - Information System Maintenance Technician 2301 - Enlisted Frequency Manager 2379 - Transmission System Technician 2709 - Joint Force Air Component Commander (JFACC) System Administrator 2710 - Global and Command Control System-Maritime 4.X (GCCS-M 4.X) System Administrator 2730 - Naval Tactical Command Support System (NTCSS) II Manager 2735 - Journeyman Networking Core 2765 - Global Command and Control System-Maritime (4.1) Increment 2 System Administrators 2766 - Global Command and Control System-Maritime 4.0.3 (GCCS-M 4.0.3) System Administrator 2778 - Mission Distribution System Operator 2779 - Information System Security Manager 2781 - Advanced Network Analyst 2783 - Submarine Local Area Network (SUBLAN) Technician 2790 - Information Systems Technician (IAT I) 2791 - Information Systems Administrator (IAT II) 9136 - Tactical Exploitation System (TES) Operator 9150 - Maritime Cryptologic Systems (Ship's Signal Exploitation Equipment – SSEE) Operator 9605 - Naval Modular Automated Communications Systems II (NAVMACS II) Maintenance Technician 9613 - Naval Special Warfare (NSW) Communications Technician"

Appendix 1:

Management Response from Department of the Navy Chief Information Officer

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

24 April 2014

MEMORANDUM FOR ASSISTANT AUDITOR GENERAL OF THE NAVY FOR FINANCIAL MANAGEMENT AND COMPTROLLER AUDITS

Subj: NAVAUDSVC DRAFT AUDIT REPORT 2012-052, 1 APRIL 2014, "CYBERSPACE/INFORMATION TECHNOLOGY SKILL SETS FOR ACTIVE DUTY MILITARY PERSONNEL AT SELECTED NAVY COMMANDS"

Ref: (a) NAVAUDSVC Draft Audit Report, Cyberspace/Information Technology Skill Sets for Active Duty Military Personnel at Selected Navy Commands

Encl: (1) DON CIO Response to Naval Audit Service Report 2012-052

Per reference (a), this memorandum forwards the Department of the Navy Chief Information Officer's (DON CIO) response to the Naval Audit Service (NAVAUDSVC) report 2012-052, "Cyberspace/Information Technology Skill Sets for Active Duty Military Personnel at Selected Navy Commands."

Findings 1-3 and recommendations 1-4, 10 and 11, which applied to the DON CIO, are addressed in enclosure (1). The DON CIO concurs with all NAVAUDSVC recommendations. The Deputy Chief of Naval Operations (Information Dominance) (OPNAV N2/N6) is responding under separate correspondence to finding number 2 and recommendations 5-9.

The DON CIO point of contact for this matter is [redacted] FOIA (b)(6)

[redacted] FOIA (b)(6)
Department of the Navy
Chief Information Officer

Copy to:
NAVAUDGEN (Attn: [redacted]) FOIA (b)(6)
NAVINSGEN N14

RECOMMENDATIONS AND FINDINGS – DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICE RESPONSE TO NAVAL AUDIT SERVICE REPORT 2012-052

NAVAUDSVC Findings: Findings 1 – 3 pertain to identification, administration, and training of Cyberspace/Information Technology Workforce as well as the use of the Managers' Internal Control Program to assess Cyberspace workforce programs.

DON CIO Response: Concur. This audit validates the need for actions already underway within the Department of the Navy. Its findings and recommendations support the actions that the DON CIO, Navy and Marine Corps are taking to transition to the Cyberspace Workforce concept.

RECOMMENDATIONS:

NAVAUDSVC Recommendation 1: Develop and issue guidance to convey to the members of the DON Cyberspace/Information Technology Workforce their inclusion and role within the Cyberspace/Information Technology workforce structure. At a minimum, this guidance should:

- Include all necessary information to ensure even the most junior personnel of the Cybersecurity and remaining Cyberspace/Information Technology Workforce understand that they comprise the overall Cyberspace/Information Technology Workforce.
- Require that this guidance be communicated to all levels within the Department of the Navy.

DON CIO Response: Concur. Future DoD and DON policy and guidance will address the overall "Cyberspace Workforce" in total. The DoD definitions for the Cyberspace Workforce are not approved. The draft DoD Directive 8140.aa Department of Defense (DoD) defines the "Cyberspace/Information Technology Workforce" as a subset of the overall "Cyberspace Workforce." Additionally, the Navy has established the Information Dominance Corps (IDC), which is a focused, mature workforce structure that clearly establishes a professional community. The DON CIO will work with the Navy to ensure that personnel understand their role in the Cyberspace Workforce through the issuance of revised DON policy. The DoD Directive 8140 should be released in the near future. The DON guidance will be promulgated by 30 September 2014.

NAVAUDSVC Recommendation 2: Establish workforce requirements to identify and track positions, personnel, and qualifications within the Cyberspace/Information Technology Workforce.

DON CIO Response: Concur. The DON is in the process of coding Cyberspace and Cybersecurity positions as directed by OPM memo of 8 July 2013, subj: "Special Cybersecurity Workforce Project" and DoD CIO memo of 27 Feb 2014, subj: "Coding of DoD Cyberspace Management & IT/IM Workforce" (CIO000144-14). Additionally, the DON CIO is working with the Navy and Marine Corps to determine what information is required to properly identify and track Cyberspace Workforce positions and personnel. The Assistant Secretary of the Navy, Manpower and Reserve Affairs (ASN (M&RA)), the Deputy Assistant Secretary of the Navy for Civilian Human Resources (DASN (CHR)), DON CIO and the Navy and Marine Corps are working together to ensure that manpower and personnel requirements and guidance are part of this effort. The guidance establishing Cyberspace/IT Workforce requirements to identify and track positions, personnel, and qualifications within the Cyberspace/Information Technology Workforce will be promulgated by 30 September 2014.

Enclosure (1)

NAVAUDSVC Recommendation 3: Establish and maintain a comprehensive personnel database to capture all personnel who comprise the Department of the Navy Cyberspace/Information Technology Workforce based on the established workforce requirements. As a subset, this capability must provide the ability to identify and track personnel and positions that perform Cybersecurity functions.

DON CIO Response: Concur. Both the Navy and the Marine Corps already have authoritative personnel data bases for military positions and personnel. Civilian personnel information is maintained in the Defense Civilian Personnel Data System (DCPDS). DON CIO is working with ASN (M&RA), DASN (CHR), Navy and Marine Corps to identify the most appropriate means and database for documenting Cyberspace/IT Workforce positions and personnel information. The Navy will continue to utilize the capabilities of the Total Workforce Management System (TWMS) to track Cyberspace and Cybersecurity unique data elements (those data elements not included in authoritative manpower and personnel data bases) as necessary. The Navy and Marine Corps are currently working with TWMS to modify and add more Cybersecurity data fields to meet future needs. Target date for completion is 31 December 2014.

NAVAUDSVC Recommendation 4: Develop and issue training and certification guidance for the overall Cyberspace/Information Technology Workforce. At a minimum, this guidance should:

- Identify the specific ratings, occupational codes, and work roles that comprise the overall Cyberspace/Information Technology Workforce to ensure even the most junior members of the Cybersecurity and remaining Cyberspace/ Information Technology Workforce understands they comprise the overall Cyberspace/Information Technology Workforce.
- Clearly state procedures for the training, certification, and management of the entire Department of the Navy Cyberspace/Information Technology Workforce.
- Require that this guidance be communicated to all levels within the Department of the Navy.

DON CIO Response: Concur. Also see DON CIO response to recommendation #1. The DON CIO is working with the DoD, Navy and Marine Corps to update current guidance and procedures. This includes addressing revisions to DoD and DON Information Assurance Workforce policy. The planned release for the guidance is 30 September 2014.

NAVAUDSVC Recommendation 10: Require that all Navy commands with Cyberspace/Information Technology Work Force personnel include Cyberspace/Information Technology Work Force in their assessable units for the Managers' Internal Control Programs and perform and document internal control evaluations for these assessable units using existing sources or separate evaluations, as required.

DON CIO Response: Concur. Guidance will be included in the revision of SECNAV M-5239.2, DON Information Assurance Workforce Management Manual. This manual is being updated as the "Cybersecurity Workforce Management Manual." The planned release for this guidance is 30 September 2014.

Enclosure (1)

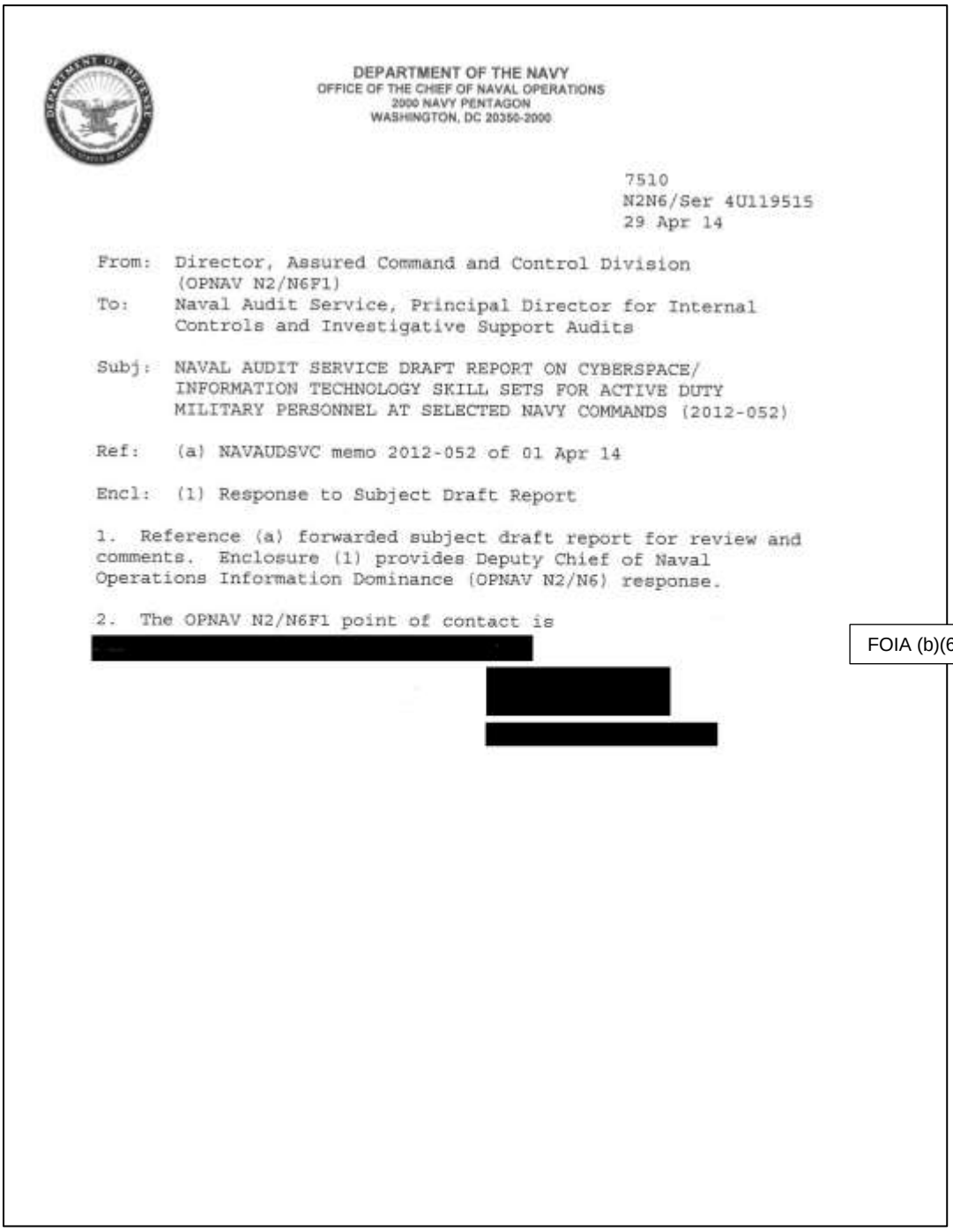
NAVAUDSVC Recommendation 11: Ensure that management at all afloat activities are aware of their responsibilities for establishing, evaluating, and improving internal controls for Cyberspace/Information Technology Workforce under the Managers' Internal Control Program.

DON CIO Response: Concur. Guidance will be included in the revision of SECNAV M-5239.2, DON Information Assurance Workforce Management Manual. This manual is being updated as the "Cybersecurity Workforce Management Manual." The planned release for this guidance is 30 September 2014.

Enclosure (1)

Appendix 2:

Management Response from Deputy Chief of Naval Operations (Information Dominance) (OPNAV N2/N6)



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

7510
N2N6/Ser 4U119515
29 Apr 14

From: Director, Assured Command and Control Division (OPNAV N2/N6F1)
To: Naval Audit Service, Principal Director for Internal Controls and Investigative Support Audits

Subj: NAVAL AUDIT SERVICE DRAFT REPORT ON CYBERSPACE/ INFORMATION TECHNOLOGY SKILL SETS FOR ACTIVE DUTY MILITARY PERSONNEL AT SELECTED NAVY COMMANDS (2012-052)

Ref: (a) NAVAUDSVC memo 2012-052 of 01 Apr 14

Encl: (1) Response to Subject Draft Report

1. Reference (a) forwarded subject draft report for review and comments. Enclosure (1) provides Deputy Chief of Naval Operations Information Dominance (OPNAV N2/N6) response.

2. The OPNAV N2/N6F1 point of contact is [redacted]

FOIA (b)(6)

DIRECTOR ASSURED COMMAND AND CONTROL DIVISION
RESPONSE TO
NAVAUDSVC DRAFT AUDIT REPORT ON
"CYBERSPACE/INFORMATION TECHNOLOGY SKILL SETS FOR ACTIVE DUTY MILITARY PERSONNEL AT SELECTED NAVY COMMANDS" 2012-052 DATED 01APR14

Finding 2: Training of Navy Cyberspace/IT Workforce Personnel

Although 93 (80 percent) of the 117 active duty Navy Cyberspace/IT Workforce (CS/ITWF) personnel reviewed said that they had sufficient training to perform their required duties, 3 officers and 21 enlisted personnel (totaling 20 percent of the 117 personnel) said they did not. Also, 89 (76 percent) of the 117 active duty personnel believe IT skill gaps exist at their ship or activity and 62 (53 percent) of the 117 personnel believed that the IT function is undermanned. In addition, although training documentation was provided for 94 (80 percent) of the 117 CS/ITWF personnel reviewed, documentation was not retained or available for 23 (20 percent) of the 117 CS/ITWF personnel. CS/ITWF personnel were not sufficiently trained and IT skill gaps existed because the Department of the Navy (DON) did not:

- Provide training and certification guidance for the overall CS/ITWF as required,
- Provide sufficient guidance defining required training for CS/ITWF line officers, nor
- Provide pipeline training[1] for the Information Systems Technician/Information Systems Technician (Subsurface) (IT/ITS) ratings.

Although DON has various systems[2] that capture some training information and documentation, DON did not have a centralized system or related procedures and internal controls to retain training and certification records for all CS/ITWF active duty members.

OPNAV N2/N6 Response: Concur

For purposes of clarity, any N2N6 response on CSWF in this document refers only to Cyber Security Work Force personnel within the Cyber Space Work Force Program. Any N2N6 reference to CSWF/IT refers only to those personnel that operate, maintain and manage IT systems, etc., resourced by OPNAV N2N6. Personnel that operate/manage Platform IT (PIT) systems or non N2N6 IT systems e.g. NALCOMIS, are outside the scope of N2N6 responsibility and therefore those specific equities are not addressed in this response. Once the Cyber Space Work Force is clearly defined by DoD and DON CIO, N2N6 will ensure appropriate workforce alignment of applicable roles and responsibilities.

OPNAV N2N6 fully recognizes the criticality and undeniable challenges associated with fielding new and continuously changing Information Technology (IT). N2N6 also understands the importance of accessibility and the necessity of IT integration in support of fleet operations,

[1] Pipeline training is the control and supervision of movement or flow of students through the training pipeline. A pipeline provides accountability and helps maintain uninterrupted flow of students. (NAVEDTRA_135C, Chap.3,section 1, para. 1.1)
[2] These systems include Fleet Management & Planning System (FLTMPS) and Total Workforce Management System (TWMS).

Enclosure (1)

DIRECTOR ASSURED COMMAND AND CONTROL DIVISION
RESPONSE TO
NAVAUDSVC DRAFT AUDIT REPORT ON
"CYBERSPACE/INFORMATION TECHNOLOGY SKILL SETS FOR ACTIVE DUTY MILITARY
PERSONNEL AT SELECTED NAVY COMMANDS" 2012-052 DATED 01APR14

DOD, the Federal government, the private sector and private citizens. However, because of the integrated nature of IP based technology and the impact it has across all warfare domains; the ease to which this technology can be accessed and manipulated by both proponents and adversaries alike, has caused Navy leadership to give serious consideration in understanding who and how this technology is being managed. As a result, OPNAV Ech1 has taken significant measures to address IT and the personnel responsible for managing IT and CSWF requirements. Specifically, OPNAVN2N6 actions have resulted in a more centralized and integrated approach in the management of IT'systems and the establishment of a Single IT Technical Authority (SPAWAR). In 2009, disparately managed IT/National Security Systems (NSS) from the HI9 Platform Sponsors were realigned to the newly established N2N6 organization. This realignment ultimately resulted in the shifting of OPNAV Manpower, Personnel and Training resources under a single DCNO for IT/NSS Acquisitions (N2N6) and will help adjudicate IT systems concerns over technical skill gaps and manpower reductions driven by "perceived" system workload efficiencies. From a training perspective, OPNAV N2N6 has taken numerous steps to improve the training for the officer and enlisted cyber workforce to include approved POM submissions for course revisions and technical upgrades. OPNAV (CNO) has also approved the "standup "of the Information Dominance Type Commander (ID TYCOM) which helps identify and drive improvements of the CSWF and address any disparities associated with non IP officers managing CSWF requirements. The ID TYCOM is scheduled to be Fully Operational Capable (FOC) in December 2014.

Recommendation 5: (OPNAV N2/N6)

Redefine training requirements for Cyberspace/Information Technology Workforce line officers to ensure that they have the education and competencies needed to support the Department of the Navy's mission, goals, and dynamic workforce structure changes. Also, ensure that Cyberspace/Information Technology Workforce line officers can provide proper oversight over enlisted Cyberspace/Information Technology Workforce.

OPNAV N2/N6 Response: Concur

OPNAV N2N6 recently approved POM resources that will restructure and provide timely technical updates and significantly increases the "time to train" for Information Professional (IP) officers attending the IP Basic course. Currently the course is optional for new IP officers and is only 4 weeks in length. However, approved funding actions have increased the length of the course from 4 to 8 weeks and will be "mandatory" for all new accession IP Officers and the timeline for implementing the new course is FY16. N2N6 is also reviewing strategies to integrate aspects of IT enlisted technical training into the IP officer pipeline for added robustness. N2N6 is also conducting internal reviews to identify student resources that would allow expanded numbers of IP officers to attend the USMC C4I Officer COI (26 Weeks). The USMC course is expeditionary focused and closely parallels the technical responsibilities of an IP officer. The issue of non-IP officers serving in CSWF management roles is an ongoing discussion being coordinated with USFFC, N2N6, the ID TYCOM and "URL/RL" community

DIRECTOR ASSURED COMMAND AND CONTROL DIVISION
RESPONSE TO
NAVAUDSVC DRAFT AUDIT REPORT ON
"CYBERSPACE/INFORMATION TECHNOLOGY SKILL SETS FOR ACTIVE DUTY MILITARY PERSONNEL AT SELECTED NAVY COMMANDS" 2012-052 DATED 01APR14

leadership. Although N2N6 recognizes that the current organizational construct is not optimal for non IP officers managing CSWF requirements, the "way-ahead" decision will be determined at Ech1 in coordination with the respective Fleet and Type Commanders. However, until a final determination is made, the N2N6 CSWF mitigation strategy will be: (1) Provide clear and unambiguous Ech1 CSWF policy guidance to all levels of the Navy enterprise; (2) Provide Commanding Officers the most knowledgeable, technically proficient and operationally sound cadre of senior enlisted IT leadership possible that will assist in the oversight and management of command CSWF/IT requirements.

In reference to changes to the IP Officer course, the expected date of implementation is May 2016. For the more immediate mitigation efforts, N2N6 responses are predicated on DON CIO's update to SECNAVINST 5239 along with the release of the DoDD 8140.aa. Once these documents have been promulgated (estimated as September 2014), OPNAV N2N6 will release a NAVADMIN that will direct the fleet to these changes and ensure implementation of all directives and instructions. Estimated release date for the NAVADMIN will be May 2015.

Recommendation 6: (OPNAV N2/N6)

Ensure Information Systems Technician/Information Systems Technician (Subsurface) Cyberspace/Information Technology Workforce enlisted personnel have pipeline training and career development reflecting current set of competencies and skills needed to perform Cyberspace/Information Technology Workforce work roles.

OPNAV N2N6 Response: Concur

The Information System Technician (Surface/Subsurface) ratings have established training pipelines that support all new IT/ITS accession requirement and the required disciplines to operate in the Cyber domain. Although the IT (Surface) rating is managed more as a generalized community of IT technical personnel, there is ongoing Flag dialogue to consider measures that potentially could restructure and reconstitute the rating. This new structure, in theory, would require specific personnel or ratings to perform independently focused/specialized IT functions using either "Core/Strand" architecture or as independently managed communities (ratings). However, because of the pervasiveness of IP technology and the inevitability of EOIP (Everything over Internet Protocol), all personnel would be expected to be trained on the basics of IP technology. Upon graduation, these personnel would then either specialize (NEC) or be integrated into separate and distinct ratings solely responsible for either RF Communications; IP Networking/System Administration; Computer Network Defense; Technical Control; Communications Admin, System Maintenance, etc. This effort is ongoing and is under review by the Navy Information Dominance (IDC) Flag Panel. The IDC Flag panel consists of Information Dominance Flag stakeholders e.g. VADM [redacted] (N2N6), VADM [redacted] (Fleet Cyber Command), RDML [redacted] (Navy Cyber Forces) (NCF) and RADM [redacted] (ONI) and RADM [redacted] (METOC). The ITS rating is responsible for managing IP based functions within the submarine Networks/Communications architecture. The ETR rating (sub communications)

FOIA (b)(6)

personnel perform RF/Baseband functions aboard submarines that would be typically performed by IT (surface) personnel. Both ratings (IT/ITS) are designated as Advanced Technical Fields and attend the initial 19 weeks of A School at the Center for Information Dominance (CID) in Corry Station. Upon graduation, select IT/ITS personnel are identified to receive follow-on NEC producing C Schools and additional training/certifications before going on to the fleet. The Information Systems Technician (Subsurface) rating was stood up in 2010 to address the unique Cyber IT requirements of the submarine LAN functions only. This requirement was previously managed by various submarine ratings (FT/ET/STS) but impaired those ratings' ability to perform their normal rating functions. To ensure proper growth and development, the IT/ITS ratings are managed by a respective OPNAV Enlisted Community Manager (ECM) responsible for the required training and career development across the entire community covering a 20 year career (cradle-to-grave). Whether IT (Surface) personnel become more specialized or not, they are always at the cutting edge of new technology advancements and were targeted to participate in a recently completed 2 year DARPA research project to identify and assess the significance of Artificial Intelligence in a Learning Environment. DARPA, OPNAV N1 and N2N6 funded the concept which is designed to significantly increase the knowledge/technical level (6 Sigma gain) of randomly selected Information Systems Technician (IT) students. This DARPA project developed an Intelligent Tutor that achieved its stated goals and received personal acknowledgement from the Chief of Naval Operations (CNO) for N2N6 to implement this training technology into the IT A school ASAP. The Navy is actively working with industry to acquire this intelligent tutor capability. Once a commercial service contract is signed with Navy, new accession students could begin training in this new technology as early as October 2014.

The identified IDC Flag Panel that is reviewing the Information Systems Technician Rating way ahead and is expected to decide on a course of action by Oct 2014. The date for implementation of the DARPA/Intelligent Tutor training in the IT 'A' school is dependent upon the commercial service contract, which is scheduled to be completed by October 2014 and students will begin training by January 2015.

Recommendation 7: (OPNAV N2/N6)

Establish a centralized system to track and maintain a complete training history for Cyberspace/Information Technology Workforce personnel. This system should ensure that all source data systems which maintain electronic training and certification records are readily identifiable, and that training and certification records are maintained in cases for which records are not recorded on other systems.

OPNAV N2/N62 Response: Concur

Since the initial date of this audit, Navy has made significant strides in how it identifies, manages, trains and tracks CSWF personnel and SECNAVINST 5239 facilitates Navy internal CSWF management standards. The Total Workforce Management System (TWMS) is currently

DIRECTOR ASSURED COMMAND AND CONTROL DIVISION
RESPONSE TO
NAVAUDSVC DRAFT AUDIT REPORT ON
"CYBERSPACE/INFORMATION TECHNOLOGY SKILL SETS FOR ACTIVE DUTY MILITARY
PERSONNEL AT SELECTED NAVY COMMANDS" 2012-052 DATED 01APR14

identified as the Navy's primary CSWF management enterprise data system of choice and as previously cited in DON CIO response to NAVAUDSVC Recommendation 3; However, the iterative Ech1 and Functional Area Manager (FAM) process known as Application and Rationalization (APPRAT) will address the continued usability, supportability, and any duplication of effort concerns between TWMS and other approved Workforce management Programs of Record (POR) for purposes of long term sustainability. In the interim, TWMS will be used as the enterprise management tool for capturing required CSWF data. Ongoing improvements to TWMS are being made to remove any known gaps or system shortcomings.

In a parallel but unrelated effort and at the direction of the Chief of Naval Operations (CNO), OPNAV N2N6 instituted the first ever Cyber Integrated Readiness Assessment (IRA) which identify current and future readiness posture of a specific Warfare Domain (Cyber). The IRA is influenced by data pulled from the Defense Readiness Reporting System Navy (DRRS-N) and mandates unit reporting on specific command readiness attributes known as Readiness Pillars. Operational units report the status of their "Personnel, Equipment, Supply, Training, and Ordinance (PESTO) pillars semi-annually to CNO via the IRA. Although initial IRA analysis of the Cyber Domain identified that not all activities are reporting all aspects of their cyber posture, it is expected that succeeding iterations of this DRRS-N process will help facilitate 100% reporting and compliance. The Cyber (Assured C2) IRA is expected to be an excellent adjunct reporting tool in support of CSWF posture and TWMS. Upon further review and approval by OPNAV N2N6 Flag leadership, a NAVADMIN message will be released to the fleet that will address the current ambiguity surrounding the CSWF and reinforce the applicability of SECNAV 5239 requirements across the Navy enterprise.

DON CIO's release of the updated SECNAVINST will detail the extent that TWMS will be utilized as a tracker of the Cyber Space Work Force. Following that release as mentioned under recommendation 5 will be the N2N6 NAVADMIN detailing the requirements to fully populate TWMS with all CSWF personnel. Expected goal date of May 2015.

Recommendation 8: (OPNAV N2/N6)

Establish procedures and related internal controls requiring that electronic or hard copy training records and certifications be retained for all Cyberspace/Information Technology Workforce active duty military members as required by SECNAV Manual M-5210.1, "Department of the Navy Records Management Program, Records Management Manual".

OPNAV N2/N6 Response: Concur

Per the requirements as cited in DOD 8570.1 and SECNAV 5239, N2N6 is actively coordinating with DON CIO, Fleet Cyber Command/10th Fleet, the newly established Information Dominance TYCOM (Navy Cyber Forces Command) and Fleet TYCOMs to ensure the required internal controls are understood and properly documented by all stakeholders. We are also reviewing

DIRECTOR ASSURED COMMAND AND CONTROL DIVISION
RESPONSE TO
NAVAUDSVC DRAFT AUDIT REPORT ON
"CYBERSPACE/INFORMATION TECHNOLOGY SKILL SETS FOR ACTIVE DUTY MILITARY
PERSONNEL AT SELECTED NAVY COMMANDS" 2012-052 DATED 01APR14

applicable Air, Surface, Subsurface and Expeditionary Force Readiness Training Manuals (FRP/FRTP) and applicability of Cyber Security Inspection Program (CSICP) and Command Cyber Readiness Inspections (CCRI) to ensure unit network security management and "inspection ready" criteria for CSWF is properly understood, in place and reported. N2N6 is also reviewing the Information System Security Manager (IT 2779) Information Assurance Manager (IAM) course of instruction for applicability to activity level enforcement of MICP requirements. These actions, in conjunction with the IRA, release of the previously mentioned CSWF NAVADMIN, annual General Military Training (GMT), etc., will ensure that all unit CO, Command IAM, crew and individual CSWF personnel are aware and knowledgeable of the SECNAV MICP 5200 checklist and administrative requirements to document and track CSWF/IT personnel.

This recommendation will also be utilizing the previously mentioned NAVADMIN, goal release date of May 2015.

Recommendation 9: (OPNAV N2/N6)

Until the centralized system is established as recommended in Recommendation 7, establish procedures and related internal controls requiring that all Cyberspace/Information Technology Workforce training records and certifications be recorded/entered into the Fleet Management and Planning System or Total Workforce Management System as required.

OPNAV N2/N6 Response: Concur

TWMS is the interim enterprise management tool that Navy will use for identifying, tracking and managing CSWF personnel. As previously stated, the iterative Ech1 and Functional Area Manager (FAM) process known as Application and Rationalization (APPRAT) will address any usability, supportability or duplication of effort concerns that might exist between TWMS and other approved Workforce management Programs of Record (POR) in terms of long term viability and sustainability.

Further review of existing policy and discussions with DON CIO indicates additional SECNAV policy is forth coming to address internal controls management requirement for CSWF personnel. In the interim, N2N6 intends to address this issue in the NAVADMIN (pending Flag approval) that will speak to the specifics and identification of CSWF personnel, required management policy, procedures and training requirements as identified in the prior responses. As an additional data metric, N2N6 also intends to track the reporting of CSWF management requirement by individual unit reporting via DRRS-N and the applicable Cyber IRA. N2N6 is also reviewing this requirement with the CID Learning Center to ensure it is being addressed sufficiently in the Information Systems Security Managers (ISSM) course that trains CSWF Information Assurance Managers (IAMs).

6

DIRECTOR ASSURED COMMAND AND CONTROL DIVISION
RESPONSE TO
NAVAUDSVC DRAFT AUDIT REPORT ON
"CYBERSPACE/INFORMATION TECHNOLOGY SKILL SETS FOR ACTIVE DUTY MILITARY PERSONNEL AT SELECTED NAVY COMMANDS" 2012-052 DATED 01APR14

This recommendation will be utilizing the before mentioned NAVADMIN, goal release date of May 2015. In addition the ISSM course review will take place by November 2014, and corrections or addition of the training topics of CSWF in totality that will include documenting, tracking and record management of the work force.

FREEDOM OF INFORMATION ACT (FOIA) MARKING: The report has been reviewed and found that it does not contain any Privacy Act or other information exempt from release under FOIA.

7

Use this page as

BACK COVER

for printed copies

of this document